



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

## Header 4

[List View](#)**General Information** [Contact](#) [Default Values](#) [Discount](#) [Document Information](#) [Clarification Request](#)

Procurement Folder: 1369290


Procurement Type: Central Master Agreement

Vendor ID: VS0000037191 

Legal Name: NETWORKING FOR FUTURE INC

Alias/DBA:

Total Bid: \$106,731.00

Response Date: 03/28/2024 

Response Time: 2:02

Responded By User ID: KevinReith 

First Name: Kevin

Last Name: Reith

Email: kreith@nffinc.com

Phone: 2023049030

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 4

Total of All Attachments: 4



Department of Administration  
 Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

**State of West Virginia  
 Solicitation Response**

<b>Proc Folder:</b>	1369290	
<b>Solicitation Description:</b>	Network Penetration Testing and Cybersecurity Assessments	
<b>Proc Type:</b>	Central Master Agreement	
<b>Solicitation Closes</b>	<b>Solicitation Response</b>	<b>Version</b>
2024-03-28 13:30	SR 0705 ESR03272400000005484	1

<b>VENDOR</b>
VS0000037191 NETWORKING FOR FUTURE INC

**Solicitation Number:** CRFQ 0705 LOT2400000009

**Total Bid:** 106731      **Response Date:** 2024-03-28      **Response Time:** 02:02:01

**Comments:** \*\* SPECIAL DISCOUNT TERMS \*\*  
 NFF will offer a 15% discount if all four years are contracted up-front (i.e. WV-Lottery provides a Purchase Order for all 4 years, rather than a Purchase Order for one year, with Option Years added-on each year thereafter)

**FOR INFORMATION CONTACT THE BUYER**  
 Brandon L Barr  
 304-558-2652  
 brandon.l.barr@wv.gov

<b>Vendor Signature X</b>	<b>FEIN#</b>	<b>DATE</b>
-------------------------------	--------------	-------------

**All offers subject to all terms and conditions contained in this solicitation**

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				17788.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** \*\* EXTERNAL NETWORK PENETRATION TESTING \*\*  
 This is the price for one (1) Assessment with all the Deliverables as noted in the RFQ Bid requirements. NFF is partnering with Cisco TALOS Advanced Services for this endeavor, and has been providing this service for over 15 years.  
 This price is all-inclusive for the description of services and deliverables requested under RFQ section 4.1  
 Note: This amount is referenced in the "UNIT COST" column of the EXHIBIT A - PRICING PAGE.  
 The PRICING PAGE has a "TOTAL BID AMOUNT" of \$853,848.00

**Extended Description:**  
 See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				17788.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** \*\* WEBSITE PENETRATION TESTING \*\*  
 This is the price for one (1) Assessment with all the Deliverables as noted in the RFQ Bid requirements. NFF is partnering with Cisco TALOS Advanced Services for this endeavor, and has been providing this service for over 15 years.  
 This price is all-inclusive for the description of services and deliverables requested under RFQ section 4.2  
 Note: This amount is referenced in the "UNIT COST" column of the EXHIBIT A - PRICING PAGE.  
 The PRICING PAGE has a "TOTAL BID AMOUNT" of \$853,848.00

**Extended Description:**  
 See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				22871.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** \*\* INTERNAL/CLIENT-SIDE NETWORK PENETRATION TESTING \*\*  
 This is the price for one (1) Assessment with all the Deliverables as noted in the RFQ Bid requirements. NFF is partnering with Cisco TALOS Advanced Services for this endeavor, and has been providing this service for over 15 years.  
 This price is all-inclusive for the description of services and deliverables requested under RFQ section 4.3  
 Note: This amount is referenced in the "UNIT COST" column of the EXHIBIT A - PRICING PAGE.  
 The PRICING PAGE has a "TOTAL BID AMOUNT" of \$853,848.00

**Extended Description:**  
 See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				48284.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** \*\* WIRELESS PENETRATION TESTING \*\*

This is the price for one (1) Assessment with all the Deliverables as noted in the RFQ Bid requirements. NFF is partnering with Cisco TALOS Advanced Services for this endeavor, and has been providing this service for over 15 years.

This price is all-inclusive for the description of services and deliverables requested under RFQ section 4.4

Note: This amount is referenced in the "UNIT COST" column of the EXHIBIT A - PRICING PAGE.

The PRICING PAGE has a "TOTAL BID AMOUNT" of \$853,848.00

**Extended Description:**

See Attached Specifications and Exhibit - A Pricing Page



Department of Administration  
 Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

**State of West Virginia  
 Centralized Request for Quote  
 Service - Prof**

**Proc Folder:** 1369290  
**Doc Description:** Network Penetration Testing and Cybersecurity Assessments  
**Proc Type:** Central Master Agreement

**Reason for Modification:**

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

**BID RECEIVING LOCATION**

BID CLERK  
 DEPARTMENT OF ADMINISTRATION  
 PURCHASING DIVISION  
 2019 WASHINGTON ST E  
 CHARLESTON WV 25305  
 US

**VENDOR**

**Vendor Customer Code:**  
**Vendor Name :**  
**Address :**  
**Street :**  
**City :**  
**State :** **Country :** **Zip :**  
**Principal Contact :**  
**Vendor Contact Phone:** **Extension:**

**FOR INFORMATION CONTACT THE BUYER**

Brandon L Barr  
 304-558-2652  
 brandon.l.barr@wv.gov

**Vendor Signature X** *Kevin J Reith* **FEIN#** **DATE**

**All offers subject to all terms and conditions contained in this solicitation**

**ADDITIONAL INFORMATION**

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached.

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON US	WV	CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

**Extended Description:**  
See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON US	WV	CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

**Extended Description:**  
See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Internal/Client-Side Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

**Extended Description:**  
See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

**Extended Description:**  
See Attached Specifications and Exhibit - A Pricing Page

**SCHEDULE OF EVENTS**

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions due by 10:00am ET	2024-03-21



## **INSTRUCTIONS TO VENDORS SUBMITTING BIDS**

**1. REVIEW DOCUMENTS THOROUGHLY:** The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

**2. MANDATORY TERMS:** The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

**3. PREBID MEETING:** The item identified below shall apply to this Solicitation.

A pre-bid meeting will not be held prior to bid opening

A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

**4. VENDOR QUESTION DEADLINE:** Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline:

Submit Questions to:  
2019 Washington Street, East  
Charleston, WV 25305  
Fax: (304) 558-3970  
Email:

**5. VERBAL COMMUNICATION:** Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

**6. BID SUBMISSION:** All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wvOASIS*, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wvOASIS* at its sole discretion. Such a prohibition will be contained and communicated in the *wvOASIS* system resulting in the Vendor's inability to submit bids through *wvOASIS*. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in *wvOASIS* are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

**For Request for Proposal ("RFP") Responses Only:** Submission of a response to a Request for Proposal is not permitted in *wvOASIS*. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus \_\_\_\_\_ convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**Bid Delivery Address and Fax Number:**

Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, WV 25305-0130  
Fax: 304-558-3970

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:

BUYER:

SOLICITATION NO.:

BID OPENING DATE:

BID OPENING TIME:

FAX NUMBER:

**7. BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time:

Bid Opening Location: Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, WV 25305-0130

*\* We acknowledge (1) addendum*

**8. ADDENDUM ACKNOWLEDGEMENT:** Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

**9. BID FORMATTING:** Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

**10. ALTERNATE MODEL OR BRAND:** Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

**11. EXCEPTIONS AND CLARIFICATIONS:** The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

**12. COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

**13. REGISTRATION:** Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the \$125 fee, if applicable.

**14. UNIT PRICE:** Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

**15. PREFERENCE:** Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: [www.state.wv.us/admin/purchase/vrc/Venpref.pdf](http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf).

**15A. RECIPROCAL PREFERENCE:** The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: [www.state.wv.us/admin/purchase/vrc/Venpref.pdf](http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf).

**16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:** For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

**17. WAIVER OF MINOR IRREGULARITIES:** The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

**18. ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

**19. NON-RESPONSIBLE:** The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance.”

**20. ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b.”

**21. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**22. WITH THE BID REQUIREMENTS:** In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

**23. EMAIL NOTIFICATION OF AWARD:** The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor wvOASIS or the Purchasing Division's website to determine when a contract has been awarded.

**24. ISRAEL BOYCOTT CERTIFICATION:** Vendor's act of submitting a bid in response to this solicitation shall be deemed a certification from bidder to the State that bidder is not currently engaged in, and will not for the duration of the contract, engage in a boycott of Israel. This certification is required by W. Va. Code § 5A-3-63.

## **GENERAL TERMS AND CONDITIONS:**

**1. CONTRACTUAL AGREEMENT:** Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

**2. DEFINITIONS:** As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

**2.1. "Agency" or "Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

**2.2. "Bid" or "Proposal"** means the vendors submitted response to this solicitation.

**2.3. "Contract"** means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

**2.4. "Director"** means the Director of the West Virginia Department of Administration, Purchasing Division.

**2.5. "Purchasing Division"** means the West Virginia Department of Administration, Purchasing Division.

**2.6. "Award Document"** means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

**2.7. "Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

**2.8. "State"** means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

**2.9. "Vendor" or "Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

**3. CONTRACT TERM; RENEWAL; EXTENSION:** The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

**Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of \_\_\_\_\_  
\_\_\_\_\_. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as \_\_\_\_\_), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

**Renewal Term:** This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to \_\_\_\_\_ successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Alternate Renewal Term** – This contract may be renewed for \_\_\_\_\_ successive \_\_\_\_\_ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Delivery Order Limitations:** In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

**Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within \_\_\_\_\_ days.



**Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within \_\_\_\_\_ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

the contract will continue for \_\_\_\_\_ years;

the contract may be renewed for \_\_\_\_\_ successive \_\_\_\_\_ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

**One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

**Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as \_\_\_\_\_), and continues until the project for which the vendor is providing oversight is complete.

**Other:** Contract Term specified in \_\_\_\_\_

**4. AUTHORITY TO PROCEED:** Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

**5. QUANTITIES:** The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

**Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

**Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

**Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

**One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

**Construction:** This Contract is for construction activity more fully defined in the specifications.

**6. EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute a breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

**7. REQUIRED DOCUMENTS:** All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

**LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

**8. INSURANCE:** The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

**Commercial General Liability Insurance** in at least an amount of: \_\_\_\_\_ per occurrence.

**Automobile Liability Insurance** in at least an amount of: \_\_\_\_\_ per occurrence.

**Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: \_\_\_\_\_ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

**Commercial Crime and Third Party Fidelity Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Cyber Liability Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

**Pollution Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Aircraft Liability** in an amount of: \_\_\_\_\_ per occurrence.

**9. WORKERS' COMPENSATION INSURANCE:** Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

**10. VENUE:** All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

**11. LIQUIDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

\_\_\_\_\_ for \_\_\_\_\_.

Liquidated Damages Contained in the Specifications.

Liquidated Damages Are Not Included in this Contract.

**12. ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

**13. PRICING:** The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

**14. PAYMENT IN ARREARS:** Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

**15. PAYMENT METHODS:** Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

**16. TAXES:** The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

**17. ADDITIONAL FEES:** Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

**18. FUNDING:** This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

**19. CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

**20. TIME:** Time is of the essence regarding all matters of time and performance in this Contract.

**21. APPLICABLE LAW:** This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

**22. COMPLIANCE WITH LAWS:** Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**23. ARBITRATION:** Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

**24. MODIFICATIONS:** This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

**25. WAIVER:** The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

**26. SUBSEQUENT FORMS:** The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

**28. WARRANTY:** The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

**29. STATE EMPLOYEES:** State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

**30. PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in [www.state.wv.us/admin/purchase/privacy](http://www.state.wv.us/admin/purchase/privacy).

**31. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

**DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.**

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**32. LICENSING:** In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

**34. VENDOR NON-CONFLICT:** Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

**35. VENDOR RELATIONSHIP:** The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

**36. INDEMNIFICATION:** The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

**37. NO DEBT CERTIFICATION:** In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

**38. CONFLICT OF INTEREST:** Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.



**39. REPORTS:** Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at [purchasing.division@wv.gov](mailto:purchasing.division@wv.gov).

**40. BACKGROUND CHECK:** In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

**41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS:** Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.
- c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
  1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
  2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

**42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL:** In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a “substantial labor surplus area”, as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

**43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE:** W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**44. PROHIBITION AGAINST USED OR REFURBISHED:** Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

**45. VOID CONTRACT CLAUSES:** This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

**46. ISRAEL BOYCOTT:** Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) \_\_\_\_\_

(Address) \_\_\_\_\_

(Phone Number) / (Fax Number) \_\_\_\_\_

(email address) \_\_\_\_\_

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

\_\_\_\_\_  
(Company) *Kevin J. Reith*  
\_\_\_\_\_  
(Signature of Authorized Representative)

\_\_\_\_\_  
(Printed Name and Title of Authorized Representative) (Date)

\_\_\_\_\_  
(Phone Number) (Fax Number)

\_\_\_\_\_  
(Email Address)

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**SPECIFICATIONS**

- 1. PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery (Lottery) to establish a contract to perform and deliver information technology cybersecurity assessments, including external network, website, wireless, and internal/client-side penetration testing assessments. These assessments must follow the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. The services provided must thoroughly assess and evaluate the Lottery infrastructure to identify areas that present an exploitable vulnerability available to attackers using a combination of automated tools and manual techniques.

**BACKGROUND INFORMATION:**

- The Lottery expects to consume at least one of each service annually.
- Physical instruction and Text Smishing are not in scope for these services.
- Source code will not be provided.
- A password analysis is not required.
- Retesting after vulnerabilities are remediated is out of scope. Each assessment stands alone.
- Sampling approaches are prohibited.
- Written information security policies are not in scope.

**EXISTING TECHNOLOGY ENVIRONMENT:** The following is a listing of the Lottery's current technology environment:

- The Lottery operates technology assets in eight (8) locations:
  - Main Office – 900 Pennsylvania Ave, Charleston, WV 25302
  - Bridgeport – 64 Sterling Drive, Bridgeport, WV 26330
  - Weirton – 100 Municipal Plaza Bldg. 34, Weirton, WV 26330
  - Greenbrier – 101 W. Main Street, White Sulphur Springs, WV 24986
  - Hollywood – 750 Hollywood Drive, Charles Town, WV 25414
  - Mardi Gras – 1 Greyhound Drive, Cross Lanes, WV 25313
  - Mountaineer – 1420 Mountaineer Circle, New Cumberland, WV 26047
  - Wheeling Island – 1 Stone Street, Wheeling, WV 26003
- One (1) externally accessible website hosted by a third party
- One (1) Active Directory domain
- Two (2) external IP address blocks, 15 external IP addresses (approximate)
- 27 internal IP address blocks, 500 internal IP addresses (approximate)
- 200 active users (approximate)

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- Cisco network devices (approximate)
  - 10 Firewall appliances
  - 15 Routers
  - 35 Switches
  - 4 VPN appliances
- 250 Windows operating system endpoints, various versions
- 120 Voice over IP (VOIP) phones
- 40 Windows servers, various versions
  - These are replicated to redundant servers at the hot site
- Two (2) Linux storage appliances
- 30 Networked Printers with onboard operating systems and storage

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 **“Contract Items”** means the information technology cybersecurity assessments as more fully described in these specifications in Section 3.1 below and on the Pricing Page.

2.2 **“Pricing Pages”** means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A and used to evaluate the Solicitation responses.

2.3 **“Solicitation”** means the official notice of an opportunity to supply the State with goods or services published by the Purchasing Division.

2.4 **“Holidays”** means days designated by WV State Code CSR 2-2-1 as legal holidays.

2.5 **“NDA”** means Non-Disclosure Agreement, attached hereto as Exhibit B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.

2.6 **“Reconnaissance”** means passively gathering as much information about the Lottery infrastructure as possible to build attack profiles. During this phase, efforts are made to map identifying information about the infrastructure.

2.7 **“Mapping”** means activities that facilitate an understanding of the lottery's business logic, flow, and organization.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 2.8 “Discovery”** means actively probing the Lottery to identify vulnerabilities at various operational layers.
- 2.9 “Exploitation”** means the Culmination of the information gathered in the previous phases to verify and confirm any identified vulnerabilities.
- 2.10 “External Network Penetration Test”** means an iterative, four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide. It comprises activities to identify vulnerabilities of externally available hosts accessible from the Internet. Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.
- 2.11 “Website Penetration Testing”** means an iterative, four-phased assessment employing techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project to verify the Lottery website security status independently. This assessment determines whether websites present an exploitable risk to the organization. Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.
- 2.12 “Internal/Client Side Network Penetration Testing”** means an iterative, four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide, comprising activities to identify vulnerabilities at each operational layer of the target network. This includes two-part testing to assess the security of all networked assets, including but not limited to servers, desktops, firewalls, other network devices, and network monitoring & management. Part one simulates an attack by an untrusted outsider or an unauthenticated user without working knowledge of the Lottery's network. Part two will be performed with the low-level credentials of an authenticated user.
- 2.13 “Wireless Network Penetration Testing”** means an iterative, four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide. It comprises activities to identify vulnerabilities at each target wireless network operational layer.
- 2.14 “DoS”** means Denial of Service, an attack that occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.
- 2.15 “SAN”** means Storage Area Network is a specialized, high-speed network that provides block-level network access to storage.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 2.16 “PTES”** means Penetration Testing Execution Standard and consists of the initial communication and reasoning behind a pen test, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it
- 2.17 “CISSP”** means Certified Information Systems Security Professional certification granted by the International Information System Security Certification Consortium.
- 2.18 “GPEN”** means GIAC Penetration Tester certification validates a practitioner's ability to properly conduct a penetration test using best-practice techniques.
- 2.19 “OSCP”** means Offensive Security Certified Professional hands-on penetration testing certification, requiring holders to successfully attack and penetrate various live machines in a safe lab environment.
- 2.20 “CEH”** means Certified Ethical Hacker is a qualification given obtained by demonstrating knowledge of assessing the security of computer systems.
- 2.21 “CPTE”** means Certified Penetration Testing Engineer presents information based on the 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting.
- 2.22 “CEPT”** means Certified Expert Penetration Tester, has deep knowledge of web hacking techniques and methodologies.
- 2.23 “CRTOP”** means Certified Red Team Operations Professional uses tactics, techniques, and procedures that threat actors use to infiltrate IT systems and stay under the detection radar.
- 2.24 “ECSA”** means Certified Security Analyst an advanced security certification that complements the Certified Ethical Hacker (CEH) certification by validating the analytical phase of ethical hacking.
- 2.25 “CPPT”** means Certified Professional Penetration Tester utilizes a variety of methodologies to conduct a thorough penetration test, and write a complete report as part of the evaluation.
- 2.26 “CWSP”** means Certified Wireless Security Professional an advanced level certification that measures the ability to secure any wireless network.



REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**2.27 “CMWAPT”** means Certified Mobile and Web Application Penetration Tester certification using pen testing methodologies and tools to conduct tests on Web and mobile apps and asses their security.

**3. QUALIFICATIONS:** Vendor, or Vendor’s staff, if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

**3.1** The vendor must have been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments.

**3.1.1** Vendor should provide, with their bid, a general company overview that must include information regarding the professional services offered and the number of dedicated security staff resources.

**3.2** Vendor should provide, with their bid, a minimum of three (3) references for projects of similar or greater size and scope of the assessments to be performed for the Lottery.

**3.2.1** References shall include contact information and brief details of the services performed for each reference.

**3.3** Vendor should provide, with their bid, an overview of the project team and documentation of qualifications for each project team member assigned to Lottery cybersecurity assessments.

**3.3.1** Documentation shall consist of information regarding the prior security assessments completed, resumes, and documentation of certifications, which should be provided as stated below in section 3.4.

**3.4** Vendor staff performing information technology cybersecurity assessments must hold a current certification from a source of accreditation and should provide the certification credentials with their bid response. Allowable certifications include:

**3.4.1** Certified Information Systems Security Professional (CISSP)

**3.4.2** GIAC Penetration Tester (GPEN)

**3.4.3** Offensive Security Certified Professional (OSCP)

**3.4.4** Certified Ethical Hacker (CEH)

**3.4.5** Certified Penetration Testing Engineer (CPTE)

**3.4.6** Certified Expert Penetration Tester (CEPT)

**3.4.7** Certified Red Team Operations Professional (CRTOP)

**3.4.8** Certified Security Analyst (ECSA)

**3.4.9** Certified Professional Penetration Tester (CPPT)

**3.4.10** Certified Wireless Security Professional (CWSP)

**3.4.10.1** This certification is only applicable to Wireless Penetration Testing Services

**3.4.11** Certified Mobile and Web Application Penetration Tester (CMWAPT)

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**3.4.11.1** This certification is only applicable to Website Penetration Services

**3.5** Vendor must comply with the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

**3.6 Background Checks:** Prior to award and upon request, the Vendor must provide names, addresses, and fingerprint information for a law enforcement background check for any Vendor staff working on the Lottery project team.

**3.7 Non-Disclosure Agreement (NDA):** Prior to award both parties, the Vendor and Lottery must sign a mutual Non-Disclosure Agreement (NDA), attached as Exhibit – B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.

#### **4. MANDATORY REQUIREMENTS:**

##### **4.1. External Network Penetration Testing**

**4.1.1.** External Network Penetration Testing may be performed remotely.

**4.1.2.** Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

**4.1.3.** Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

###### **4.1.3.1.Reconnaissance should include:**

**4.1.3.1.1.** Perform WHOIS, ARIN, and DNS (public server) lookups

**4.1.3.1.2.** OSINT - Public Searches/Dorks

**4.1.3.1.3.** Build custom password lists

**4.1.3.1.4.** DNS lookups (entities server)

**4.1.3.1.5.** Gather information from entities network resources

**4.1.3.1.6.** Analyze metadata

###### **4.1.3.2.Mapping should include:**

**4.1.3.2.1.** Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.)

**4.1.3.2.2.** Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports)

**4.1.3.2.3.** OS/Version Scanning (Identify underlying OS and software and their versions)

###### **4.1.3.3.Discovery should include:**

**4.1.3.3.1.** Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 4.1.3.3.2. Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.)
- 4.1.3.3.3. Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)
- 4.1.3.4. Exploitation should include:**
  - 4.1.3.4.1. Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)
  - 4.1.3.4.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)
  - 4.1.3.4.3. Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the penetration test steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).
- 4.1.4. Must identify exploitable vulnerabilities and demonstrate organizational impact.
- 4.1.5. Denial of service (DoS) attacks are prohibited for External Network Penetration Testing services.
- 4.1.6. A social engineering exercise must be included. This will consist of a single phishing email scenario targeting approximately 200 active Lottery staff. The content must be designed to maximize successful phishing, and the email content and target addresses must be verified and approved by the Lottery.
- 4.1.7. Heavy load brute force or automated attacks will only be performed with prior Lottery approval.
- 4.1.8. Must notify Lottery of any portion or portions of the assessment resulting in service disruption.
- 4.1.9. The Lottery must be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.
- 4.1.10. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
  - 4.1.10.1. The vendor shall provide a sample of the executive summary report with their bid response.
  - 4.1.10.2. The report must be submitted to the Lottery electronically for review.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 4.1.11. Upon conclusion of the assessment the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.
- 4.1.12. Reports must include specific details for each vulnerability found, including:
  - 4.1.12.1. How the vulnerability was discovered
  - 4.1.12.2. The potential impact of its exploitation.
  - 4.1.12.3. Recommendations for remediation.
  - 4.1.12.4. Vulnerability references
  - 4.1.12.5. The vendor shall provide a sample of the technical report with their bid response.
  - 4.1.12.6. The report must be submitted to the Lottery electronically for review.
- 4.1.13. Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.
  - 4.1.13.1 The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

#### **4.2. Website Penetration Testing**

- 4.2.1. Website Penetration Testing may be performed remotely.
- 4.2.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
- 4.2.3. The successful vendor must determine static and dynamic page counts.
- 4.2.4. Any environment, such as production, development, quality assurance, etc., may be tested. Each environment will be assessed separately.
- 4.2.5. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
  - 4.2.5.1. Reconnaissance should include:**
    - 4.2.5.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups
    - 4.2.5.1.2. OSINT - Public Searches/Dorks
    - 4.2.5.1.3. Build custom password lists
    - 4.2.5.1.4. DNS lookups (entities server)
    - 4.2.5.1.5. Gather information from entities web applications
    - 4.2.5.1.6. Analyze metadata
  - 4.2.5.2. Mapping should include:**
    - 4.2.5.2.1. SSL/TLS Analysis (Identify accepted SSL/TLS ciphers)
    - 4.2.5.2.2. Virtual Hosting & Load Balancer Analysis

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 4.2.5.2.3. Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.)
- 4.2.5.2.4. HTTP Options Discovery (Identify accepted HTTP methods)
- 4.2.5.2.5. Web Application Spidering (gather/follow all links)
- 4.2.5.2.6. Directory Browsing (Identify web directory listings, brute force common web directory names)
- 4.2.5.2.7. Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app)
- 4.2.5.2.8. Session Analysis (Identify locations where session cookies are set and analyze predictability)
- 4.2.5.3. Discovery should include:**
  - 4.2.5.3.1. Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)
  - 4.2.5.3.2. Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)
  - 4.2.5.3.3. Identify Web Application Specific/Web Service Specific Vulnerabilities (Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc.)
  - 4.2.5.3.4. Identify Authentication/Authorization Issues/Bypasses (Weak access control, weak password policy, session management, etc.)
- 4.2.5.4. Exploitation should include:**
  - 4.2.5.4.1. Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)
  - 4.2.5.4.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)
  - 4.2.5.4.3. Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the pentest steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).
- 4.2.6. Must provide identification of prioritized remediation needs, requirements, and associated risks.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 4.2.7.** Testing shall determine if website vulnerabilities exist by testing each website, including server operating systems, application platforms, and databases.
- 4.2.8.** Denial of Service (DoS) attacks are required for Website Penetration Testing and require notification to the Lottery and Lottery approval before the attack commences.
- 4.2.9.** Heavy load brute force or automated attacks will only be performed with prior Lottery approval.
- 4.2.10.** Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
  - 4.2.10.1.** The vendor shall provide a sample of the executive summary report with their bid response.
  - 4.2.10.2.** The report must be submitted to the Lottery electronically for review.
- 4.2.11.** Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.
- 4.2.12.** Reports must include specific details for each vulnerability found, including:
  - 4.2.12.1.** How the vulnerability was discovered
  - 4.2.12.2.** The potential impact of its exploitation.
  - 4.2.12.3.** Recommendations for remediation.
  - 4.2.12.4.** Vulnerability references
  - 4.2.12.5.** The vendor shall provide a sample of the technical report with their bid response.
  - 4.2.12.6.** The report must be submitted to the Lottery electronically for review.
- 4.2.13.** Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.
  - 4.2.13.1.** The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**4.3. Internal/Client-Side Network Penetration Testing**

- 4.3.1. Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.
- 4.3.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
- 4.3.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
  - 4.3.3.1. **Reconnaissance should include:**
    - 4.3.3.1.1. Identify software versions along with potentially useful software configurations or settings
    - 4.3.3.1.2. Identify any anti-malware, firewall, and IDS products on the system
    - 4.3.3.1.3. Gather information about the network (i.e., domain user/group information, domain computers, password policy)
    - 4.3.3.1.4. Verify the ability to execute scripts or third-party programs
  - 4.3.3.2. **Mapping and Discovery should include:**
    - 4.3.3.2.1. Identify possible vulnerabilities affecting the provided host
    - 4.3.3.2.2. Determine the possibility of receiving and executing various malicious payloads
  - 4.3.3.3. **Exploitation should include:**
    - 4.3.3.3.1. Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges
    - 4.3.3.3.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)
- 4.3.4. Must identify prioritized remediation needs, requirements, and associated risks.
- 4.3.5. Testing shall assess the security of all networked assets, including but not limited to servers, endpoints, firewalls, network devices, and network monitoring and management.
- 4.3.6. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
  - 4.3.6.1. Vendor shall provide a sample of the executive summary report with their bid response.
  - 4.3.6.2. Report must be submitted to Lottery electronically for review.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 4.3.7. Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.
- 4.3.8. Reports must include specific details for each vulnerability found, including:
  - 4.3.8.1. How the vulnerability was discovered.
  - 4.3.8.2. The potential impact of its exploitation.
  - 4.3.8.3. Recommendations for remediation.
  - 4.3.8.4. Vulnerability references.
  - 4.3.8.5. The vendor shall provide a sample of the technical report with their bid response.
  - 4.3.8.6. The report must be submitted to the Lottery electronically for review.
- 4.3.9. Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.
  - 4.3.9.1. The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

#### 4.4. Wireless Penetration Testing

- 4.4.1. Wireless Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.
- 4.4.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
- 4.4.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
  - 4.4.3.1. **Reconnaissance should include:**
    - 4.4.3.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups
    - 4.4.3.1.2. OSINT - Public Searches/Dorks
    - 4.4.3.1.3. Build custom password lists
    - 4.4.3.1.4. DNS lookups (entities server)
    - 4.4.3.1.5. Gather information from entities web applications
    - 4.4.3.1.6. Analyze metadata
  - 4.4.3.2. **Mapping should include:**
    - 4.4.3.2.1. Sniffing (establish a baseline of traffic, sniff Wi-Fi, Bluetooth, Zigbee, and other RF)
    - 4.4.3.2.2. War Walk (map location of access points and their coverage, identify leakage)
    - 4.4.3.2.3. Identify Rogue Access Points\* (Friendly, malicious, or unintended access points)



REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

- 4.4.3.2.4. Full access to the buildings will be granted to the testing team
- 4.4.3.3. **Discovery should include:**
  - 4.4.3.3.1. Identify Points of Attack (Identify WEP networks, capture WPA/WPA2 PSK key exchanges, identify clients for evil-twin and MiTM attacks)
  - 4.4.3.3.2. Enumerating Services (Connect and interact with services on APs, Bluetooth Devices, and other RF devices to disclose misconfigurations)
  - 4.4.3.3.3. Vulnerability Scanning (Identify vulnerabilities)
- 4.4.3.4. **Exploitation should include:**
  - 4.4.3.4.1. AP Attacks (Exploit hotspots, perform MiTM attacks, crack WEP, crack WPA/WPA2 PSK, etc.)
  - 4.4.3.4.2. Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.)
  - 4.4.3.4.3. Denial of Service where applicable and with prior Lottery approval
  - 4.4.3.4.4. Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval
- 4.4.4. Must identify prioritized remediation needs, requirements, and associated risks.
- 4.4.5. Testing shall assess the security of all wireless assets.
- 4.4.6. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
  - 4.4.6.1. Vendor shall provide a sample of the executive summary report with their bid response.
  - 4.4.6.2. Report must be submitted to Lottery electronically for review.
- 4.4.7. Upon completing the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered and assigns a critical, high, medium, or low risk rating.
- 4.4.8. Reports must include specific details for each vulnerability found, including:
  - 4.4.8.1. How the vulnerability was discovered.
  - 4.4.8.2. The potential impact of its exploitation.
  - 4.4.8.3. Recommendations for remediation.
  - 4.4.8.4. Vulnerability references.
  - 4.4.8.5. The vendor shall provide a sample of the technical report with their bid response.
  - 4.4.8.6. The report must be submitted to the Lottery electronically for review.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**4.4.9.** Upon the conclusion of the assessment, the Vendor must present a Findings Presentation to the Lottery management team. This presentation shall provide an overview of the strengths, weaknesses, and vulnerabilities identified throughout the assessment.

**4.4.9.1.** The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**5. CONTRACT AWARD:**

**5.1 Contract Award:** The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the Vendor that provides the Network Penetration Testing and Cybersecurity Assessments meeting the required specifications for the lowest total bid amount as shown on the Pricing Pages.

**5.2 Pricing Page:** Vendor should complete the Pricing Page by entering the unit cost per assessment and reports as a fixed amount for all penetration testing, vulnerability assessments, reports and findings presentation to calculate the extended amount. Then add all extended amount line items together to get the total bid amount. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

The Pricing Page contains an estimated number for assessments. The estimates represent an amount that will be utilized for evaluation purposes only. No future use of the Contract or any individual item is guaranteed or implied.

Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document. In most cases, the Vendor can request an electronic copy of the Pricing Pages for bid purposes by sending an email request to the following address: [brandon.l.barr@wv.gov](mailto:brandon.l.barr@wv.gov)

**6. PERFORMANCE:** Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

7. **PAYMENT:** Agency shall pay the hourly rate, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.
8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.
9. **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:
  - 9.1. Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
  - 9.2. Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
  - 9.3. Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
  - 9.4. Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
  - 9.5. Vendor shall inform all staff of Agency's security protocol and procedures.
10. **VENDOR DEFAULT:**
  - 10.1. The following shall be considered a vendor default under this Contract.
    - 10.1.1. Failure to perform Contract Services in accordance with the requirements contained herein.
    - 10.1.2. Failure to comply with other specifications and requirements contained herein.
    - 10.1.3. Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.
    - 10.1.4. Failure to remedy deficient performance upon request.

REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**10.2.** The following remedies shall be available to Agency upon default.

**10.2.1.** Immediate cancellation of the Contract.

**10.2.2.** Immediate cancellation of one or more release orders issued under this Contract.

**10.2.3.** Any other remedies available in law or equity.

**11. MISCELLANEOUS:**

**11.1. Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

**Contract Manager:** \_\_\_\_\_  
**Telephone Number:** \_\_\_\_\_  
**Fax Number:** \_\_\_\_\_  
**Email Address:** \_\_\_\_\_

**EXHIBIT A - Pricing Page**

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$ -	\$ -
2	4.2	Website Penetration Testing	8	\$ -	\$ -
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ -	\$ -
4	4.4	Wireless Penetration Testing	8	\$ -	\$ -
<b>TOTAL BID AMOUNT</b>					\$ -

**\*Please note the following information is being captured for auditing purposes and is an estimate for evaluation only\***

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	
Vendor Address:	
Email Address:	
Phone Number:	
Fax Number:	
Signature and Date:	<i>Steve Hancock</i>

**EXHIBIT B**  
**NON-DISCLOSURE AGREEMENT (NDA)**

**MUTUAL NON-DISCLOSURE AGREEMENT**

This Mutual Non-Disclosure Agreement (“Agreement”) is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 (“Lottery”), and \_\_\_\_\_, with its principal offices located at \_\_\_\_\_ (“Party of the second part”), with an Effective Date of \_\_\_\_\_. Lottery and Party of the second party also are referred to herein individually as a “party”, or collectively as the “parties”.

WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain information or communication technology services by one party of interest to the other party; and

WHEREAS, the parties agree that improper disclosure of either party’s Confidential Information, as defined below, by the other party could cause material harm to the party whose Confidential Information was improperly disclosed;

NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and Alpha agree to maintain the confidentiality of the Confidential Information as follows:

**I. Definition of Confidential Information.** The "Confidential Information" disclosed under this Agreement is defined as follows:

Any data or information that is proprietary to the disclosing party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, intellectual property, and trade secrets; (v) solicitation for proposals, responses to proposals, bids, or information disclosed in connection with such solicitation, response, or bid; (vi) any other information that should reasonably be recognized as confidential information of the disclosing party.

**II. Disclosure Period and Term.** This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party’s performance of its obligations associated with that certain CRFQ Agreement executed between the parties on \_\_\_\_\_ (the “Effective Date”) and 3 year(s) after the termination of such Agreement (“Disclosure Period”). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

**EXHIBIT B**  
**NON-DISCLOSURE AGREEMENT (NDA)**

Period. Upon termination of this Agreement or upon the disclosing party's request, the recipient shall cease use of Confidential Information and return or destroy it.

- III. Use of Confidential Information.** A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.
- IV. Protection of Confidential Information.** Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.
- V. Exclusions.** This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.
- VI. Miscellaneous.** Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.
- VII. Export Administration.** Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.
- VIII. No Obligation to Purchase or Offer Products or Services.** Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

**EXHIBIT B  
NON-DISCLOSURE AGREEMENT (NDA)**

the other party. Neither party has an obligation under this Agreement to commercially offer any products using or incorporating the Confidential Information. The disclosing party may, at its sole discretion, offer such products commercially and may modify them or discontinue such offerings at any time.

**IX. General.** The parties do not intend that any agency or partnership relationship be created between them by this Agreement. This Agreement sets forth the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements concerning such Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. This Agreement and all matters arising out of or relating to this Agreement shall be governed by the laws of the State of West Virginia. The parties agree that the information provided as allowed by this Agreement will not contain any proprietary technical or confidential contractual information, or any financial information related to the relationship between Alpha and its partners. As a result, damages will not be included as a remedy.

The undersigned authorized representatives of each party have agreed to be legally bound by the terms of this Agreement as of the Effective Date shown above.

**WEST VIRGINIA LOTTERY**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

\_\_\_\_\_ **(VENDOR)**

By: Steve Hancock \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_





# WV Lottery - Network Penetration Testing & Assessment Services RFP

## Proposal for WV Lottery

March 30, 2024





## Disclaimer - Cisco Systems, Inc.

The information contained in this proposal is proprietary and confidential to Cisco Systems, Inc. (hereafter "Cisco") and is furnished in confidence with the understanding that it will not, without the express written permission of Cisco, be used or disclosed for other than proposal evaluation purposes.

This is not an offer to contract with Cisco. Please note that Cisco is making this proposal with the understanding that if you desire to purchase the Cisco products and services described in Cisco's main response to the proposal, you will select an authorized Cisco reseller as the prime contractor. In that event, your contract with your selected reseller will govern the terms and conditions of your purchase, including all pricing. Cisco cannot, in any fashion, dictate or control resale pricing. For further information about Cisco's authorized resellers, please see: [www.cisco.com/en/US/partners/index.html](http://www.cisco.com/en/US/partners/index.html). Any reference to "partner" in this proposal is not intended to imply any equity relationship, investment or creation of a partnership interest for legal purposes.

If you ultimately decide to purchase the products and/or services described in this proposal directly with Cisco, then all terms and conditions (inclusive of all business terms and conditions) will be pursuant only to a final and definitive written agreement between the customer and Cisco. A final written agreement will embody the exclusive statement of the agreement between the customer and Cisco as it relates to the sale of products and services by Cisco occurring on or after the effective date of the agreement and will take the form of (a) Cisco's standard Terms of Sale (a copy of which is available at: [www.cisco.com/legal](http://www.cisco.com/legal)), (b) an existing and applicable written agreement in effect between the customer and Cisco, (including any amendments), if applicable, or (c) a mutually negotiated final written agreement (individually and collectively the "Final Agreement"). For purposes of clarity, for a direct relationship with Cisco, the Final Agreement will replace all other terms and conditions, and Cisco hereby takes exception to all other terms and conditions. If at the time of the award no such agreement has been executed, and customer decides to purchase products and services from Cisco, then all such purchases will be subject to Cisco's then-current Terms of Sale.

Cisco may have provided certain direct pricing information in this proposal; however all such pricing is provided by Cisco for your convenience and budgetary purposes only, and does not constitute a bid or an offer from Cisco. Further, Cisco makes no representations, warranties or covenants in this proposal (including without limitation as to any products, services, service levels, third-party products or services or interoperability). Any information provided in this proposal regarding future functionalities is for informational purposes only and is subject to change including ceasing any further development of such functionality. Many of these future functionalities remain in varying stages of development and will be offered on a when-and-if available basis, and Cisco makes no commitment as to the final delivery of any of such future functionalities. Cisco will have no liability to customer for Cisco's failure to delivery any or all future functionalities and any such failure would not in any way imply the right to return any previously purchased Cisco products.

Financial information about Cisco, including annual and quarterly reports, can be found at the Cisco Investor Relations homepage, which provides a link to the company's most recent filings with the Securities and Exchange Commission (SEC): <http://investor.cisco.com>. As Cisco is a public company and is required to disclose its financial status on a quarterly and annual basis; the reports filed with the SEC are available in lieu of any requested credit and/or bank references.

This proposal is valid for a period of ninety (90) days from the date of this proposal's submission.



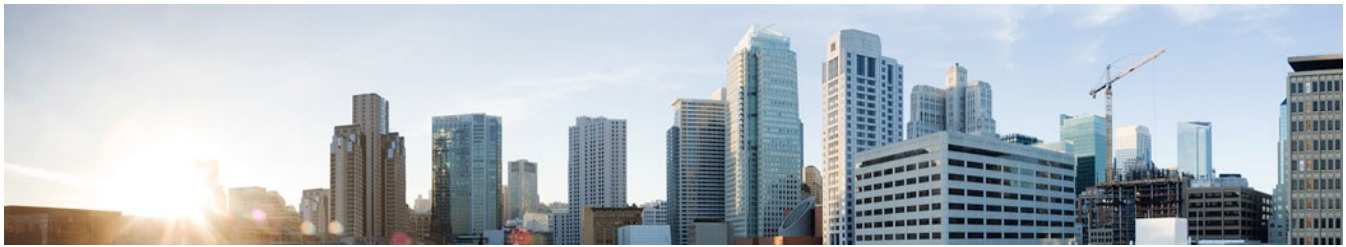
---

# Table of Contents

<b>1. EXECUTIVE SUMMARY.....</b>	<b>3</b>
<b>STATEMENT OF COMPLIANCE .....</b>	<b>5</b>



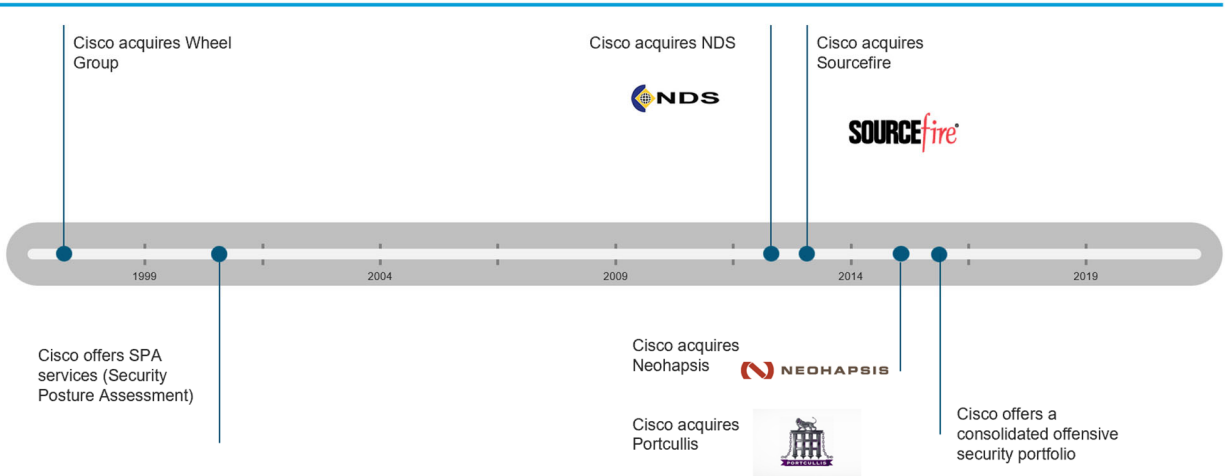
# 1. Executive Summary



We are pleased to present our proposal for the Cisco Technical Security Assessment Service Offering. Our team at WV Lottery is committed to providing comprehensive, proactive, and effective security solutions to protect your organization's digital assets.

For over a quarter of a century, Cisco has been delivering security assessment services to our clientele. In 2015, we expanded our focus on these services by acquiring two companies specializing in security assessments, namely Neohapsis and Portcullis. At present, our global team consists of more than 50 security assessment engineers, with a significant presence in the United States and the United Kingdom. Additionally, we have established four hardware labs worldwide, including two in the United States, to ensure comprehensive assessment coverage from the smallest chip to the expansive cloud.

## A Short History of Penetration Testing at Cisco



In the last decade, our assessment and penetration testing team has carried out over 6000 assessments, identifying more than 177,000 security vulnerabilities. This equates to an average of approximately 32 issues identified per assessment.



Our Cisco Technical Security Assessment Service Offering includes:

1. **Detailed Security Assessment:** Our certified Cisco security experts will conduct a thorough analysis of your network infrastructure, applications, and endpoints. We will use advanced tools and methodologies to identify potential vulnerabilities and areas for improvement.
2. **Review of Security Policies and Procedures:** We will evaluate your existing security policies and procedures to ensure they are robust and effective.
3. **Penetration Testing:** Our team will conduct penetration testing to identify any vulnerabilities that could be exploited by cybercriminals.
4. **Risk Analysis:** We will provide a comprehensive risk analysis to help you understand the potential threats to your organization and how to mitigate them.
5. **Compliance Evaluation:** We will assess your organization's compliance with relevant industry standards and regulations.
6. **Detailed Report:** Upon completion of the assessment, we will provide a detailed report outlining our findings and recommendations for improving your security posture. This will include suggested Cisco security solutions tailored to your specific needs.

Our team has extensive experience in conducting security assessments and implementing Cisco security solutions. We have successfully helped numerous organizations enhance their security posture and protect their digital assets.

We look forward to the opportunity to work with you and contribute to the security of your organization. If you have any questions or require further information, please do not hesitate to contact us.

Thank you for considering our proposal.



## Statement of Compliance

### 3. QUALIFICATIONS: Vendor, or Vendor's staff, if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1. The vendor must have been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments.

3.1.1. Vendor should provide, with their bid, a general company overview that must include information regarding the professional services offered and the number of dedicated security staff resources.

#### **Cisco response:**

Cisco has been providing security assessment services to our customers for over 25 years. In 2015, Cisco acquired two security companies focused on security assessment services, Neohapsis and Portcullis. Currently Cisco has over 50 security assessment engineers around the globe, with large concentrations in the United States and the United Kingdom. Moreover, we have four hardware labs positioned globally, including two in the United States, to ensure that assessment coverage is covered from chip to cloud.

Over the past 10 years, Cisco's assessment and penetration testing team has conducted over 6000 assessments uncovering more than 177,000 security gaps, with ~32 issues discovered per assessment.

The concept of solutions being driven to address specific customer challenges has been with Cisco since its inception. Cisco was started in 1984 by a husband-and-wife team, Len Bosack and Sandy Lerner, who were involved in running Stanford University's computer operations. They developed a multiprotocol router to send each other e-mail across the campus, even though each used a different computer system.

Cisco engineers have been prominent in advancing the development of IP, the basic language to communicate over the Internet and in private networks. As the Internet grew in the mid-1990s, Cisco routers served as the core infrastructure for the Internet.

Today, Cisco designs and sells broad lines of products, provides services, and delivers integrated solutions to develop and connect networks around the world, building the Internet. Through our decades in business, we have been the world's leader in connecting people, things, and technologies - to each other and to the Internet - realizing our vision of changing the way the world works, lives, plays and learns.

We have over 85,000 employees in over 95 offices worldwide who design, produce, sell, and deliver integrated products, services, and solutions. Over time, we have expanded to new markets that are a natural extension of our core networking business, as the network has become the platform for automating, orchestrating, integrating, and delivering an ever-increasing array of information technology (IT)-based products and services.

We conduct our business globally and manage our business by geography. Our business is organized into the following three geographic segments: The Americas; Europe, Middle East, and Africa (EMEA); and Asia Pacific, Japan, and China (APJC).

Our products and technologies are grouped into the following categories: Infrastructure Platforms; Applications; Security and Other Products. In addition to our product offerings, we provide a broad range



of service offerings, including technical support services and advanced services. Increasingly, we are delivering our technologies through software and services. Our customers include businesses of all sizes, public institutions, governments, and service providers. These customers often look to us as a strategic partner to help them use information technology (IT) to differentiate themselves and drive positive business outcomes.

At Cisco, our customers come first and an integral part of our CISCO DNA is creating long-lasting customer partnerships and collaborating with them to identify their needs and provide solutions that support their success.

For more information, please visit: <https://newsroom.cisco.com/c/r/newsroom/en/us/company.html>

Cisco offers an extensive portfolio of professional services that support all stages of the lifecycle. These stages include Architecture, Planning, Design, Implementation, Testing, Operations, and Optimization. These services are designed to help businesses effectively utilize Cisco's technology solutions.

3.2. Vendor should provide, with their bid, a minimum of three (3) references for projects of similar or greater size and scope of the assessments to be performed for the Lottery.

3.2.1. References shall include contact information and brief details of the services performed for each reference.

**Cisco response:**

Please note that the identity of Cisco clients is considered confidential information. Because of confidentiality agreements, it is Cisco's policy not to provide contact names or references on an initial information response. However, Cisco is more than happy to arrange reference calls and visits as we move further along in the engagement with WV Lottery.

Recent Client Engagements:

**Large Auto Manufacturer**

- **Challenge:** Large auto manufacturer considering the introduction of "Phone-as-a-Key" as a feature potentially replacing traditional vehicle authentication methods.
- **Solution:** Cisco Security Services Application Threat Modeling and Design Review.
- **Outcomes:** Cisco uncovered several new critical threats that had not been considered during design. Unaddressed threats would enable easy theft of vehicles.

**Top tier video game publisher**

- **Challenge:** Top-tier video game publisher wanted to estimate how long it would take a skilled attacker to pirate their new title distributed through Steam for PC.
- **Solution:** Cisco Security Services Penetration Testing.
- **Outcomes:** Cisco evaluated the attack surface and identified the DRM software boundary. Cisco used runtime process instrumentation to intercept DRM calls and fake responses. The title was cracked in 3 weeks.



## Large technology Company

- **Challenge:** Large technology company was migrating internal applications to a hybrid cloud environment, leveraging AWS.
- **Solution:** Cisco's Cloud Application Security Services and Purple Team Services
- **Outcomes:** Cisco enumerated critical design threats and discovered weaknesses in the deployment of the application and the AWS configuration. Cisco worked to address these weaknesses and maximize the application along with the AWS configuration. Cisco also worked to maximize the investment in AWS through native and bespoke security controls. Moreover, Cisco leveraged its Purple Team services to improve SOC processes and train personnel on detection.

For general customer success stories, please visit: <https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories.html>.

3.3. Vendor should provide, with their bid, an overview of the project team and documentation of qualifications for each project team member assigned to Lottery cybersecurity assessments.

3.3.1. Documentation shall consist of information regarding the prior security assessments completed, resumes, and documentation of certifications, which should be provided as stated below in section 3.4.

### Cisco response:

Over the past 10 years, Cisco's assessment and penetration testing team has conducted over 6000 assessments uncovering more than 177,000 security gaps, with ~32 issues discovered per assessment.

Cisco would assign a project team at the time of signed based on availability and skillset. The following are examples of biographies from our assessment and penetration testing team:

## Security Consultant

### Areas of Expertise

- Red Team
- Physical Security Assessments
- Security Incident Management
- Integrating Security into Agile SDLC
- Social Engineering
- Network Penetration Testing
- Application Back Box Testing

Consultant Name Sanitized is a Security Consultant with over eight years' experience in information security. He is a generalist with experience in working with development teams, infrastructure teams, and executive leadership to educate and lead change. His expertise includes network infrastructure security, incident response and security program and compliance management.





## Key Projects

- Designed an Agile SDLC integration strategy for an online marketing company attempting to move to Agile methods and continuous integration delivery with timeline for delivery based on the capabilities of the teams involved and the security needs of the organization.
- Served on the application security staff of a Fortune 500 company performing assessments of new applications and helped manage the vulnerability management process.
- Performed social engineering assessments targeting employees within an organization and sending targeted spear phishing messages.
- Performed on-site and remote third-party security risk assessments.
- Performed red team, external and internal penetration tests for companies in the following sectors:
  - eCommerce
  - Social Media
  - Real Estate
  - Content Hosting
  - Managed Services
  - Gaming
- Performed black box assessments of various application types including:
  - Payment API's
  - Regulated form workflows
  - Remote support applications
  - Social media applications
  - Linux video games
- Built and implemented a security information program for a research division of a university.
- Primary forensic investigator for a breach involving hundreds of servers and clients.

## Previous Professional Experience

**Northwestern University, Kellogg School of Management**  
Chief Security Officer (Senior Data Security Analyst)

Evanston, IL  
2007 – 2014

Consultant Name Sanitized served as Chief Security Officer and the primary resource for Information Security. He built a risk-based security program and led projects to achieve security objectives for a university's division of with over 6,000 students, faculty, and staff. He led the institution's response to security breaches and educated constituents and leadership on security and compliance issues. Consultant Name Sanitized managed the school's PCI compliance obligations and led efforts to remove unnecessary personal information from enterprise systems to individual laptops.

In addition, Consultant Name Sanitized worked closely with IT staff developing and improving internal incident response and building patch management programs for servers and client systems. He audited and managed the replacement of old firewalls and brought in log management systems so that they could be monitored. He performed security architecture, network assessments, and black box reviews of internal and contracted projects.



**Northwestern University, Kellogg School of Management**  
Senior IT Consultant

Evanston, IL  
2006 – 2007

Consultant Name Sanitized lead the client systems technical team for the rollout of Windows Vista, Office 2007, and Exchange 2007 to the school. He led the creation of a new imaging system, managed consulting resources, selected hardware and software configuration, and designed testing plans. In addition, he mentored support staff, handled escalated problems from the help desk, and led the support response to complex technical issues involving external vendors and internal teams.

**Northwestern University, Kellogg School of Management**  
Public Computing Manager

Evanston, IL  
2001 – 2006

Consultant Name Sanitized managed public computing facilities on multiple campuses throughout North America. He also managed renovation projects and day-to-day operations of equipment and staff.

### Education

**Northwestern University**  
B.S. in Mechanical Engineering

Evanston, IL  
1996 – 2001

### Certifications

**CISSP 2006**  
Active

**GSEC 2005**  
Inactive

## Senior Security Consultant

### Areas of Expertise

- Web Application Penetration Testing
- Application Design Assessments
- Application Development
- Network Penetration Testing
- Third Party Assessments

Consultant serves as a Senior Security Consultant in Cisco's Security Services. Joining Cisco in 2015 as part of the Neohapsis acquisition, he brings over 15 years of security consulting experience with strengths in application security and a software development background. Consultant has assessed a variety of security and application technologies, many of which have required creative approaches to assess, and often in team-oriented environments. Pat's role is not simply to deliver services, but also to help people better understand security.



## Key Projects

### Fortune 100 Financial Services Provider

- Conducted blackbox and penetration testing of consumer-targeted web applications that deliver and support innovative retail payment technologies and cash transfers.
- Supported provider's incident response activities.
- Developed written reports disclosing risks, vulnerabilities, and recommended remedial actions.
- Made additional recommendations to improve the overall security stance of technologies in use.

### Fortune 1000 Software Technology Developer

- Assessed major components of vendor's web technology portfolio for vulnerabilities and potential risks. Technologies included web media asset development, management, and presentation platforms and a popular web server platform featuring numerous functional components.

### Cloud Services Provider – Storage

- Conducted blackbox application penetration testing of retail and corporate cloud storage services, including client and server components, to identify vulnerabilities that disclose data or provide access to functionality.

### Cloud Services Provider – SaaS

- Assessed in depth a suite of enterprise-level SaaS applications including ERP, HRIS, and CRM applications.
- Assessed deployment platform for low-level vulnerabilities.
- Conducted application penetration testing against application functionality.

### Home Automation Services

- Assessed home automation devices for vulnerabilities in authorization and communications protocols.
- Performed additional blackbox and grey-box testing of provider's web applications to support and manage the devices

### Certificate Authority

- Assessed the security of applications and processes that support both retail and wholesale issuance of PKI certificates used by a global client base to provide secure (SSL) communication with customers and B2B partners.

### Application Service Provider – Medical

- Conducted penetration tests for applications storing Protected Healthcare Information (PHI) belonging to patients numbering in the millions, including Electronic Health Record and PACS applications.



### Third Party Maturity Assessment

- Assessed third party vendors using an ISO-based approach to ascertain levels of organizational and process maturity across a range of analysis areas.
- Identified gaps and made recommendations for improvement.

### Third Party Technology Assessment

- Assessed third-party application technologies using blackbox assessment techniques.
- Used customer and industry requirements to assist in assessing level of risk posed by technologies.
- Identified vulnerabilities and made recommendations for mitigation to reduce risk of exploit in customer environments.

## Professional Experience

**Symantec** Boston, MA  
Lead Technical Architect 2004-2008

As a consultant at Symantec, Consultant delivered application security assessment services to corporate clients in the financial services, healthcare, retail, marketing, education, and manufacturing industries. In addition, Pat's role as lead of the Application Security Center of Excellence helped expand both the breadth of the consulting organization's technical knowledge, as well as overall delivery capacity by training and mentoring others.

**@stake** Boston, MA  
Managing Security Architect 2000-2004

Pat's application development experience increased the breadth of expertise at security services pioneer @stake, where he participated in the development and delivery of security assessment services in an industry that was awakening to these needs. The resulting services were a key asset in the firm's ultimate acquisition by Symantec Corp. Corporate clients belonged to verticals that included financial services, utilities, healthcare, publishing, education, and manufacturing.

**Open Market, inc.** Burlington, MA  
Software Principal Engineer 1996-2000

As member and eventual lead of the Security Team, Consultant helped specify, develop, and maintain the security feature set for the company's flagship line of internet commerce and server products, including Open Market Transact.

## Education

**Cornell University** Ithaca, NY  
BS in Computer Science, College of Engineering 1988



## Senior Security Consultant

### Areas of Expertise

- Web Application Security Assessment
- Network Penetration Testing
- Network Vulnerability Assessment
- Application Design Assessment
- Network Architecture Assessment
- Linux Server Hardening Assessment

Consultant is an accomplished information security practitioner with 22 years of information technology experience, including 18 years of primary focus on network and web application penetration testing. Consultant has delivered security assessment projects for major automotive, banking, education, energy, financial, government, healthcare, information security, insurance, retail, and technology clients. In addition, Consultant has instructed firewall and penetration testing courses and written technical blog posts.

### Key Projects

- Consultant performed a web application penetration test and Linux server hardening assessment for a major retail client. The web application penetration test was conducted against the flagship electronic commerce website, while the Linux server hardening assessment focused on Red Hat Enterprise Linux (RHEL) and Ubuntu Linux. Consultant leveraged Center for Internet Security (CIS) benchmarks in order to identify several security flaws within Linux operating system deployments.
- Consultant performed a web application penetration test and Point of Sale (POS) assessment for a major entertainment client. The assessment focused on ticketing applications and included both register and mobile POS devices. Consultant incorporated multiple attack vectors, including application business logic flaws, POS software vulnerabilities, and physical access in order to identify pervasive security flaws that could adversely affect business unit revenue.
- Consultant performed a web application penetration test of an extranet web application for a major law firm. The web application, a frontend for Microsoft SharePoint Server, was designed to store and share confidential legal information with clients. Consequently, Consultant focused his efforts on validation of Single Sign-On (SSO) authentication and robust role-based access controls in order to protect critical client information.

### Professional Experience

**@stake / Symantec**  
Senior Security Consultant

Chicago, IL  
2003-2015

Consultant performed network and web application penetration tests for a variety of clients across multiple vertical markets. For example, Consultant helped build and manage an onsite security assessment team for a major retail client. To support this initiative, Consultant developed custom security assessment process, assessment, and reporting tools. The onsite team employed eight full time employees and identified security flaws in hundreds of web applications. In addition to performing network and web application penetration tests, Consultant also conducted security research projects and instructed penetration testing courses.



### **Exault / VeriSign**

Senior Security Consultant

Chicago, IL

2000-2003

Consultant performed firewall installations and network penetration tests for a variety of clients across multiple vertical markets. For example, Consultant helped design, deploy, and maintain the firewall infrastructure for a major energy client. The firewall infrastructure integrated custom hardware and software solutions and supported mission critical SCADA communications. In addition to performing firewall installations and network penetration tests, Consultant also instructed firewall and network penetration testing courses.

### **Andersen Consulting**

Webmaster / Security Consultant

Northbrook, IL

1997-2000

Consultant functioned as the webmaster for the Andersen Consulting corporate website. Job responsibilities included research of web server technology, deployment of web server content, and security assessment of Common Gateway Interface (CGI) scripts. In addition to webmaster duties, Consultant also researched Intrusion Detection Systems (IDS) technology. Based on Consultant 1's research, Andersen Consulting procured and deployed IDS technology on crucial network segments. Furthermore, Consultant performed network penetration tests of strategic Andersen Consulting networks.

### **Speaking and Publishing**

- Consultant has instructed firewall and penetration testing courses. Consultant has also developed custom course content based on dynamic client requirements.
- Consultant has published numerous technical blog posts on prestigious websites including LinkedIn, Infosec Island, and Symantec. Topics included web and mobile application penetration testing, SQL injection, browser security tools, and web server hardening.
- Consultant has delivered multiple information security presentations at Cisco corporate and client events.

### **Education**

#### **Elmhurst College**

B.S. Computer Science & B.S. Mathematics

Elmhurst, IL

1993-1997

### **Certifications**

#### **CISSP (Certified Information Systems Security Professional) 1999**

Active

#### **GSEC (Global Information Assurance Certification Security Essentials Certification) 1999**

Inactive

#### **GCFW (Global Information Assurance Certification Certified Firewall Analyst) 1999**

Inactive

#### **CCSA (Check Point Certified Security Administrator) 2000**

Inactive



**CCSE (Check Point Certified Security Engineer) 2000**

Inactive

**CCSI (Check Point Certified Security Instructor) 2000**

Inactive

**CCNA (Cisco Certified Network Associate) 2001**

Inactive

**CCNP (Cisco Certified Network Professional) 2001**

Inactive

**SCSA (Sun Certified System Administrator) 2002**

Inactive

**SCNA (Sun Certified Network Administrator) 2002**

Inactive

We have a structured Product Management process we follow based on PMI standards. We layer on top of this a quality assurance process that includes detailed peer reviews and business reviews of any deliverables or work products.

Testers are part of a segmented team dedicated to security assessments. In addition to rigorous interview/vetting during the hiring process, we invest significantly in training. This includes shadowing, regular brown bags and tech talks, external training, and industry conference attendance. Most of the staff in this group are seasoned, with 10+ years of experience on average.

3.4. Vendor staff performing information technology cybersecurity assessments must hold a current certification from a source of accreditation and should provide the certification credentials with their bid response. Allowable certifications include:

3.4.1. Certified Information Systems Security Professional (CISSP)

3.4.2. GIAC Penetration Tester (GPEN)

3.4.3. Offensive Security Certified Professional (OSCP)

3.4.4. Certified Ethical Hacker (CEH)

3.4.5. Certified Penetration Testing Engineer (CPTE)

3.4.6. Certified Expert Penetration Tester (CEPT)

3.4.7. Certified Red Team Operations Professional (CRTOP)

3.4.8. Certified Security Analyst (ECSA)

3.4.9. Certified Professional Penetration Tester (CPPT)

3.4.10. Certified Wireless Security Professional (CWSP)

3.4.10.1. This certification is only applicable to Wireless Penetration Testing Services

3.4.11. Certified Mobile and Web Application Penetration Tester (CMWAPT)

3.4.11.1. This certification is only applicable to Website Penetration Services



**Cisco response:**

Experienced and credentialed team. Our consultants average 8 to 10 years of information security experience, and some have more than 15 years. They come from a variety of backgrounds, such as Chief Information Security Officer, vulnerability researcher, malware expert, or application developer. And most team members have one or more security or industry certifications. These include:

- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)
- SANS Global Information Assurance Certification (GIAC)
- Security Essentials (SANS GSEC)
- SANS GIAC Certified Forensic Analyst (SANS GFCA)
- Certified Penetration Testing Engineer (CPTe)
- Certified Expert Penetration Tester (CEPT)
- Certified Red Team Operations Professional (CRTOP)
- Certified Security Analyst (ECSA)
- Certified Professional Penetration Tester (CPPT)
- Certified Wireless Security Professional (CWSP)
- Certified Mobile and Web Application Penetration Tester (CMWAPT)
- Project Management Professional (PMP)
- Additional Certifications: OSCP, OSCE, OSWE, OSEE, GPEN, GXPN, HKIB's CCASP, GWAPT, CREST (various), GIAC, OSWP, GSNA, GSEC, GSNA, Cisco DevNet, Cisco CyberOps, GCFE, eCRE, CEH, Professional Cloud Security Engineer, PNPT, Security+

3.5. Vendor must comply with the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

**Cisco response:**

Our team uses a proprietary testing methodology based on various public methodologies and frameworks (e.g., PTES, OSSTMM, OWASP, NIST 800-115, MITRE ATT&CK) to ensure compliance with industry regulations (e.g., PCI, GLBA, HIPAA, SOX).





Our tool-kit primarily consists of open source (e.g., Kali Linux) and commercial security assessment tools (e.g., Nessus, Cobalt Strike, Burp Suite, Ida Pro). We have developed our own testing tools and often extend and customize public tools.

3.6. Background Checks: Prior to award and upon request, the Vendor must provide names, addresses, and fingerprint information for a law enforcement background check for any Vendor staff working on the Lottery project team.

**Cisco response:**

If required, Cisco will provide necessary background check information.

Cisco conducts background checks on anyone who requires access to Cisco facilities, electronic access (email, intranet access, etc.), or any access to Cisco's confidential, proprietary, or intellectual data. This includes pre-employment background investigations on all Cisco employees, and pre-access background investigations on all non-employees (temps, contractors, consultants, vendors, and access-only individuals).

The pre-employment screenings conducted for regular Cisco hires include:

- SSN Trace (US only)
- Criminal Felony & Misdemeanor (7-year history, as local law permits)
- Federal Criminal (US only)
- Education (highest degree claimed, excludes high school diploma)
- Employment (past 3 employers, up to last 7 years, current employer not verified)
- Prohibited Parties/OFAC

Pre-access background checks must be conducted on any non-employee who requires access to Cisco facilities, electronic access, or any access to Cisco's confidential, proprietary, or intellectual data. The Supplier is responsible for initiating the background check with one of Cisco's preferred background screening vendors and for all costs acquired in the background screening process. Cisco does not initiate nor complete background checks for non-employees. Backgrounds must be completed no earlier than 6 months prior to the non-employee's start date.

The pre-access screenings conducted for non-employees include:

- Criminal Felony & Misdemeanor (7-year history, as local law permits)
- Federal Criminal (US only)
- Prohibited Parties/OFAC

Please note that some countries are exempt from the criminal check component. These include Belgium, Brazil, Canada, Chile, Croatia, Cuba, Finland, France, Germany, Greece, Guyana, Hungary, Iran, Ireland, Italy, Japan, Kazakhstan, Netherlands, Norway, Poland, Russia (CIS), Slovenia, Sudan, Sweden, Syria, Ukraine, Venezuela.



3.7. Non-Disclosure Agreement (NDA): Prior to award both parties, the Vendor and Lottery must sign a mutual Non-Disclosure Agreement (NDA), attached as Exhibit – B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.

**Cisco response:**

Cisco will work with WV Lottery to sign a mutually agreeable NDA.

## 4. MANDATORY REQUIREMENTS:

### 4.1 External Network Penetration Testing

**Cisco response:**

Cisco acknowledges that all requirements in section 4.1 External Network Penetration Testing will be met.

4.1.1. External Network Penetration Testing may be performed remotely.

4.1.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

4.1.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

4.1.3.1. Reconnaissance should include:

4.1.3.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups

4.1.3.1.2. OSINT - Public Searches/Dorks

4.1.3.1.3. Build custom password lists

4.1.3.1.4. DNS lookups (entities server)

4.1.3.1.5. Gather information from entities network resources

4.1.3.1.6. Analyze metadata

4.1.3.2. Mapping should include:

4.1.3.2.1. Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.)

4.1.3.2.2. Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports)

4.1.3.2.3. OS/Version Scanning (Identify underlying OS and software and their versions)

4.1.3.3. Discovery should include:

4.1.3.3.1. Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)

4.1.3.3.2. Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.)

4.1.3.3.3. Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)

4.1.3.4. Exploitation should include:

4.1.3.4.1. Brute Force Logins (Using discovered username/email

4.1.3.4.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

4.1.3.4.3. Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the penetration test steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).

4.1.4. Must identify exploitable vulnerabilities and demonstrate organizational impact.

4.1.5. Denial of service (DoS) attacks are prohibited for External Network Penetration Testing services.

4.1.6. A social engineering exercise must be included. This will consist of a single phishing email scenario targeting approximately 200 active Lottery staff. The content must be designed to maximize successful phishing, and the email content and target addresses must be verified and approved by the Lottery.

4.1.7. Heavy load brute force or automated attacks will only be performed with prior Lottery approval.

4.1.8. Must notify Lottery of any portion or portions of the assessment resulting in service disruption.

4.1.9. The Lottery must be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.

4.1.10. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

4.1.10.1. The vendor shall provide a sample of the executive summary report with their bid response.

4.1.10.2. The report must be submitted to the Lottery electronically for review.

**Cisco response:**

Please see the following document for an executive summary report for External Network Penetration Testing:



External Network  
Penetration Test Rej

4.1.11. Upon conclusion of the assessment the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

4.1.12. Reports must include specific details for each vulnerability found, including:

4.1.12.1. How the vulnerability was discovered

4.1.12.2. The potential impact of its exploitation.

4.1.12.3. Recommendations for remediation.

4.1.12.4. Vulnerability references

4.1.12.5. The vendor shall provide a sample of the technical report with their bid response.



4.1.12.6. The report must be submitted to the Lottery electronically for review.

**Cisco response:**

Please see the following document for the technical report for External Network Penetration Testing:



External Network  
Penetration Test Rej

4.1.13. Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

4.1.13.1. The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**Cisco response:**

Cisco will present our findings to the Lottery in person or via a conference call.

Our reporting format includes an executive summary highlighting the key findings, overall risk profile, and recommended actions for management and stakeholders. This summary is concise and easy to understand for non-technical audiences. We also include a more detailed findings summary for technical audiences to digest. Cisco provide a detailed description of each vulnerability, including the affected component, its impact, potential attack scenarios, and recommended remediation actions. Include any relevant technical details, proof-of-concept code, or exploit scripts, if applicable. Finally, more detailed information is included in appendices. This includes any additional supporting information, such as screenshots, logs, or additional analysis performed during the penetration test.

Our reporting methodology based on the Common Vulnerability Scoring System (CVSS) v3.0 providing a structured approach to reporting and assessing vulnerabilities discovered during an engagement. We clearly identify each vulnerability discovered during the penetration test and assign a unique identifier or reference number to each vulnerability for easy reference and tracking. We then use the CVSS v3.0 scoring system to assess and quantify the severity of each vulnerability. The CVSS v3.0 scoring system evaluates vulnerabilities based on their impact and exploitability factors. Cisco assigns a CVSS base score to each vulnerability, which will range from 0.0 to 10.0. Cisco consultants then generate a CVSS vector string for each vulnerability. The vector string captures the characteristics of the vulnerability, including its access complexity, authentication requirements, and impact metrics. The vector string provides additional context and helps in understanding the vulnerability's specific attributes.

With this data, Cisco classifies the vulnerabilities into severity levels based on the CVSS score ranges. For example, you can use categories like Critical (CVSS score 9.0-10.0), High (CVSS score 7.0-8.9), Medium (CVSS score 4.0-6.9), and Low (CVSS score 0.1-3.9). This classification helps prioritize remediation efforts based on the severity of the vulnerabilities.



## 4.2. Website Penetration Testing

### Cisco response:

Cisco acknowledges that all requirements in section 4.2 Website Penetration Testing will be met.

4.2.1. Website Penetration Testing may be performed remotely.

4.2.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

4.2.3. The successful vendor must determine static and dynamic page counts.

4.2.4. Any environment, such as production, development, quality assurance, etc., may be tested. Each environment will be assessed separately.

4.2.5. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

4.2.5.1. Reconnaissance should include:

4.2.5.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups

4.2.5.1.2. OSINT - Public Searches/Dorks

4.2.5.1.3. Build custom password lists

4.2.5.1.4. DNS lookups (entities server)

4.2.5.1.5. Gather information from entities web applications

4.2.5.1.6. Analyze metadata

4.2.5.2. Mapping should include:

4.2.5.2.1. SSL/TLS Analysis (Identify accepted SSL/TLS ciphers)

4.2.5.2.2. Virtual Hosting & Load Balancer Analysis

4.2.5.2.3. Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.)

4.2.5.2.4. HTTP Options Discovery (Identify accepted HTTP methods)

4.2.5.2.5. Web Application Spidering (gather/follow all links)

4.2.5.2.6. Directory Browsing (Identify web directory listings, brute force common web directory names)

4.2.5.2.7. Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app)

4.2.5.2.8. Session Analysis (Identify locations where session cookies are set and analyze predictability)

4.2.5.3. Discovery should include:

4.2.5.3.1. Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)

4.2.5.3.2. Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)



4.2.5.3.3. Identify Web Application Specific/Web Service Specific Vulnerabilities (Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc.)

4.2.5.3.4. Identify Authentication/Authorization Issues/Bypasses (Weak access control, weak password policy, session management, etc.)

4.2.5.4. Exploitation should include:

4.2.5.4.1. Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)

4.2.5.4.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

4.2.5.4.3. Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the pentest steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).

4.2.6. Must provide identification of prioritized remediation needs, requirements, and associated risks.

4.2.7. Testing shall determine if website vulnerabilities exist by testing each website, including server operating systems, application platforms, and databases.

4.2.8. Denial of Service (DoS) attacks are required for Website Penetration Testing and require notification to the Lottery and Lottery approval before the attack commences.

4.2.9. Heavy load brute force or automated attacks will only be performed with prior Lottery approval.

4.2.10. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

4.2.10.1. The vendor shall provide a sample of the executive summary report with their bid response.

4.2.10.2. The report must be submitted to the Lottery electronically for review.

#### Cisco response:

Please see the following document for an executive summary report for Website Penetration Testing:



Sample Web  
Application Assessr

4.2.11. Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

4.2.12. Reports must include specific details for each vulnerability found, including:

4.2.12.1. How the vulnerability was discovered

4.2.12.2. The potential impact of its exploitation.

4.2.12.3. Recommendations for remediation.

4.2.12.4. Vulnerability references

- 4.2.12.5. The vendor shall provide a sample of the technical report with their bid response.
- 4.2.12.6. The report must be submitted to the Lottery electronically for review.

**Cisco response:**

Please see the following document for the technical report for Website Penetration Testing:



Sample Web  
Application Assessor

4.2.13. Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

- 4.2.13.1. The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**Cisco response:**

Cisco will present our findings to the Lottery in person or via a conference call.

Our reporting format includes an executive summary highlighting the key findings, overall risk profile, and recommended actions for management and stakeholders. This summary is concise and easy to understand for non-technical audiences. We also include a more detailed findings summary for technical audiences to digest. Cisco provide a detailed description of each vulnerability, including the affected component, its impact, potential attack scenarios, and recommended remediation actions. Include any relevant technical details, proof-of-concept code, or exploit scripts, if applicable. Finally, more detailed information is included in appendices. This includes any additional supporting information, such as screenshots, logs, or additional analysis performed during the penetration test.

Our reporting methodology based on the Common Vulnerability Scoring System (CVSS) v3.0 providing a structured approach to reporting and assessing vulnerabilities discovered during an engagement. We clearly identify each vulnerability discovered during the penetration test and assign a unique identifier or reference number to each vulnerability for easy reference and tracking. We then use the CVSS v3.0 scoring system to assess and quantify the severity of each vulnerability. The CVSS v3.0 scoring system evaluates vulnerabilities based on their impact and exploitability factors. Cisco assigns a CVSS base score to each vulnerability, which will range from 0.0 to 10.0. Cisco consultants then generate a CVSS vector string for each vulnerability. The vector string captures the characteristics of the vulnerability, including its access complexity, authentication requirements, and impact metrics. The vector string provides additional context and helps in understanding the vulnerability's specific attributes.

With this data, Cisco classifies the vulnerabilities into severity levels based on the CVSS score ranges. For example, you can use categories like Critical (CVSS score 9.0-10.0), High (CVSS score 7.0-8.9), Medium (CVSS score 4.0-6.9), and Low (CVSS score 0.1-3.9). This classification helps prioritize remediation efforts based on the severity of the vulnerabilities.



#### 4.3. Internal/Client-Side Network Penetration Testing

##### **Cisco response:**

Cisco acknowledges that all requirements in section 4.3 Internal/Client-Side Network Penetration Testing will be met.

4.3.1. Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.

4.3.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

4.3.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

4.3.3.1. Reconnaissance should include:

4.3.3.1.1. Identify software versions along with potentially useful software configurations or settings

4.3.3.1.2. Identify any anti-malware, firewall, and IDS products on the system

4.3.3.1.3. Gather information about the network (i.e., domain user/group information, domain computers, password policy)

4.3.3.1.4. Verify the ability to execute scripts or third-party programs

4.3.3.2. Mapping and Discovery should include:

4.3.3.2.1. Identify possible vulnerabilities affecting the provided host

4.3.3.2.2. Determine the possibility of receiving and executing various malicious payloads

4.3.3.3. Exploitation should include:

4.3.3.3.1. Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges

4.3.3.3.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

4.3.4. Must identify prioritized remediation needs, requirements, and associated risks.

4.3.5. Testing shall assess the security of all networked assets, including but not limited to servers, endpoints, firewalls, network devices, and network monitoring and management.

4.3.6. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

4.3.6.1. Vendor shall provide a sample of the executive summary report with their bid response.

4.3.6.2. Report must be submitted to Lottery electronically for review.

##### **Cisco response:**

Please see the following document for an executive summary report for Internal/Client-Side Network Penetration Testing:





Internal Network  
Penetration Test Re

4.3.7. Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

4.3.8. Reports must include specific details for each vulnerability found, including:

- 4.3.8.1. How the vulnerability was discovered.
- 4.3.8.2. The potential impact of its exploitation.
- 4.3.8.3. Recommendations for remediation.
- 4.3.8.4. Vulnerability references.
- 4.3.8.5. The vendor shall provide a sample of the technical report with their bid response.
- 4.3.8.6. The report must be submitted to the Lottery electronically for review.

**Cisco response:**

Please see the following document for the technical report for Internal/Client-Side Network Penetration Testing:



Internal Network  
Penetration Test Re

4.3.9. Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

- 4.3.9.1. The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**Cisco response:**

Cisco will present our findings to the Lottery in person or via a conference call.

Our reporting format includes an executive summary highlighting the key findings, overall risk profile, and recommended actions for management and stakeholders. This summary is concise and easy to understand for non-technical audiences. We also include a more detailed findings summary for technical audiences to digest. Cisco provide a detailed description of each vulnerability, including the affected component, its impact, potential attack scenarios, and recommended remediation actions. Include any relevant technical details, proof-of-concept code, or exploit scripts, if applicable. Finally, more detailed information is included in appendices. This includes any additional supporting information, such as screenshots, logs, or additional analysis performed during the penetration test.

Our reporting methodology based on the Common Vulnerability Scoring System (CVSS) v3.0 providing a



structured approach to reporting and assessing vulnerabilities discovered during an engagement. We clearly identify each vulnerability discovered during the penetration test and assign a unique identifier or reference number to each vulnerability for easy reference and tracking. We then use the CVSS v3.0 scoring system to assess and quantify the severity of each vulnerability. The CVSS v3.0 scoring system evaluates vulnerabilities based on their impact and exploitability factors. Cisco assigns a CVSS base score to each vulnerability, which will range from 0.0 to 10.0. Cisco consultants then generate a CVSS vector string for each vulnerability. The vector string captures the characteristics of the vulnerability, including its access complexity, authentication requirements, and impact metrics. The vector string provides additional context and helps in understanding the vulnerability's specific attributes.

With this data, Cisco classifies the vulnerabilities into severity levels based on the CVSS score ranges. For example, you can use categories like Critical (CVSS score 9.0-10.0), High (CVSS score 7.0-8.9), Medium (CVSS score 4.0-6.9), and Low (CVSS score 0.1-3.9). This classification helps prioritize remediation efforts based on the severity of the vulnerabilities.

#### 4.4. Wireless Penetration Testing

##### **Cisco response:**

Cisco acknowledges that all requirements in section 4.4 Wireless Penetration Testing will be met.

4.4.1. Wireless Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.

4.4.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

4.4.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

4.4.3.1. Reconnaissance should include:

4.4.3.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups

4.4.3.1.2. OSINT - Public Searches/Dorks

4.4.3.1.3. Build custom password lists

4.4.3.1.4. DNS lookups (entities server)

4.4.3.1.5. Gather information from entities web applications

4.4.3.1.6. Analyze metadata

4.4.3.2. Mapping should include:

4.4.3.2.1. Sniffing (establish a baseline of traffic, sniff Wi-Fi, Bluetooth, Zigbee, and other RF)

4.4.3.2.2. War Walk (map location of access points and their coverage, identify leakage)

4.4.3.2.3. Identify Rogue Access Points\* (Friendly, malicious, or unintended access points)

4.4.3.2.4. Full access to the buildings will be granted to the testing team

4.4.3.3. Discovery should include:



- 4.4.3.3.1. Identify Points of Attack (Identify WEP networks, capture WPA/WPA2 PSK key exchanges, identify clients for evil-twin and MiTM attacks)
- 4.4.3.3.2. Enumerating Services (Connect and interact with services on APs, Bluetooth Devices, and other RF devices to disclose misconfigurations)
- 4.4.3.3.3. Vulnerability Scanning (Identify vulnerabilities)
- 4.4.3.4. Exploitation should include:
  - 4.4.3.4.1. AP Attacks (Exploit hotspots, perform MiTM attacks, crack WEP, crack WPA/WPA2 PSK, etc.)
  - 4.4.3.4.2. Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.)
  - 4.4.3.4.3. Denial of Service where applicable and with prior Lottery approval
  - 4.4.3.4.4. Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval
- 4.4.4. Must identify prioritized remediation needs, requirements, and associated risks.
- 4.4.5. Testing shall assess the security of all wireless assets.
- 4.4.6. Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
  - 4.4.6.1. Vendor shall provide a sample of the executive summary report with their bid response.
  - 4.4.6.2. Report must be submitted to Lottery electronically for review.

**Cisco response:**

Please see the following document for an executive summary report for Wireless Penetration Testing:



Wireless\_Penetration  
\_Test\_Sample\_Report

- 4.4.7. Upon completing the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered and assigns a critical, high, medium, or low risk rating.
- 4.4.8. Reports must include specific details for each vulnerability found, including:
  - 4.4.8.1. How the vulnerability was discovered.
  - 4.4.8.2. The potential impact of its exploitation.
  - 4.4.8.3. Recommendations for remediation.
  - 4.4.8.4. Vulnerability references.
  - 4.4.8.5. The vendor shall provide a sample of the technical report with their bid response.
  - 4.4.8.6. The report must be submitted to the Lottery electronically for review.

**Cisco response:**

Please see the following document for the technical report for Wireless Penetration Testing:



Wireless\_Penetration  
\_Test\_Sample\_Report

4.4.9. Upon the conclusion of the assessment, the Vendor must present a Findings Presentation to the Lottery management team. This presentation shall provide an overview of the strengths, weaknesses, and vulnerabilities identified throughout the assessment.

4.4.9.1. The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**Cisco response:**

Cisco will present our findings to the Lottery in person or via a conference call.

Our reporting format includes an executive summary highlighting the key findings, overall risk profile, and recommended actions for management and stakeholders. This summary is concise and easy to understand for non-technical audiences. We also include a more detailed findings summary for technical audiences to digest. Cisco provide a detailed description of each vulnerability, including the affected component, its impact, potential attack scenarios, and recommended remediation actions. Include any relevant technical details, proof-of-concept code, or exploit scripts, if applicable. Finally, more detailed information is included in appendices. This includes any additional supporting information, such as screenshots, logs, or additional analysis performed during the penetration test.

Our reporting methodology based on the Common Vulnerability Scoring System (CVSS) v3.0 providing a structured approach to reporting and assessing vulnerabilities discovered during an engagement. We clearly identify each vulnerability discovered during the penetration test and assign a unique identifier or reference number to each vulnerability for easy reference and tracking. We then use the CVSS v3.0 scoring system to assess and quantify the severity of each vulnerability. The CVSS v3.0 scoring system evaluates vulnerabilities based on their impact and exploitability factors. Cisco assigns a CVSS base score to each vulnerability, which will range from 0.0 to 10.0. Cisco consultants then generate a CVSS vector string for each vulnerability. The vector string captures the characteristics of the vulnerability, including its access complexity, authentication requirements, and impact metrics. The vector string provides additional context and helps in understanding the vulnerability's specific attributes.

With this data, Cisco classifies the vulnerabilities into severity levels based on the CVSS score ranges. For example, you can use categories like Critical (CVSS score 9.0-10.0), High (CVSS score 7.0-8.9), Medium (CVSS score 4.0-6.9), and Low (CVSS score 0.1-3.9). This classification helps prioritize remediation efforts based on the severity of the vulnerabilities.



# Cisco Customer Experience



Exemplum, Inc.

External Network Penetration Test

February 16, 2022

Version 1.1

## About This Document

Document Information	
<b>Author</b>	Vince Kornacki
<b>Change Authority</b>	Cisco Systems Customer Experience APT
<b>DCP Reference</b>	XXXXXX
<b>Client Reference</b>	Exemplum, Inc.
<b>Project ID</b>	XXXXXX
<b>Task Reference</b>	External_Network_Penetration_Test_Sample

Document History			
Version	Date	Status	Comments
0.1	December 20, 2022	Draft	First Draft
1.0	December 22, 2022	Complete	Peer Review

Document Review		
Reviewer	Version	Date
Patrick Madden	0.2	December 21, 2022

This document contains and constitutes the proprietary and confidential information of Cisco ("Cisco"). It is provided to Exemplum, Inc. ("Company") subject to and in accordance with the terms of any agreement between Cisco and the Company regarding treatment of confidential information and/or licensing of proprietary information. This document also contains information that is sensitive confidential information of the Company and should be treated by representatives of the Company accordingly. This document may not be distributed by the recipient without the express permission of Cisco and the Company.

The contents of this document do not constitute legal advice. Cisco's offer of services or deliverables that relate to compliance, litigation, or other legal interests is not intended as legal counsel and should not be taken as such.

# Table of Contents

Table of Contents.....	4
1. Executive Summary.....	5
1.1 Introduction .....	5
1.2 Conclusions.....	5
1.3 Recommendations .....	5
RECOMMENDED ACTION PLAN.....	5
2. Project Summary.....	7
2.1 Project Scope .....	7
2.2 Project Teams .....	7
3. Technical Analysis .....	8
3.1 Technical Summary.....	8
3.2 Summary of Findings .....	9
STRENGTHS.....	9
WEAKNESSES .....	9
INDEX OF FINDINGS.....	12
4. Detailed Findings.....	13
Appendices.....	34
Appendix A: CVSS Vector Strings .....	34
Appendix B: Definition of Terms .....	35
.....	37



# 1. Executive Summary

---

## 1.1 Introduction

Cisco performed an External Network Penetration Test of Exemplum's Internet-facing e-commerce business unit servers. A penetration test is a type of "ethical hacking" or "intrusion testing" approach for detecting computer system vulnerabilities that malicious intruders could use to exploit a system and compromise its data. The assessment took place between December 12 and 16, 2022.

Exemplum's external networks provide remote access, product purchasing, and collaboration for the e-commerce business unit of Exemplum. The networks also contain infrastructure support systems that the e-commerce business unit depends on. The primary objective of the engagement was to determine whether an external attacker could compromise Exemplum's systems or data. Exemplum requested Cisco to place special focus on attacks which could compromise confidential customer data in the quoting and ordering system.

## 1.2 Conclusions

Cisco successfully exploited a combination of vulnerabilities to compromise proprietary manufacturing specifications, internal communications, and supporting telecommunications systems within three days of testing. Focused exploitation efforts yielded access to all the customer and financial data stored on cloud.clientx.com.

Cisco identified eight (8) findings, including one (1) Critical, two (2) High, two (2) Medium, two (2) Low, and one (1) Informational finding. During the engagement, Cisco worked with Exemplum personnel to triage each critical vulnerability. At the time of writing, the Critical finding had been addressed. Due to the sensitive data and system access obtained, Cisco considered the residual risk to be quite high.

In general, exploitation of these issues could lead to customer PII being leaked on the Internet, loss of competitive advantage, reputation loss, IP theft, and general financial loss. These issues are trivially exploitable by unsophisticated attackers, using well-known attack methods.

An investigation should occur to determine if these issues have ever been exploited. If so, an incident response team should be immediately deployed to contain the existing threat. Infrastructure and development teams should update their provisioning and development practices to avoid these issues in the future. Information security teams should update or create a vulnerability management program that will enable the organization to detect and respond to these issues on a regular basis.

## 1.3 Recommendations

### RECOMMENDED ACTION PLAN

**Control Resources Throughout Their Lifetime**

While it is important to configure systems in-line with security industry best practices at the point of commissioning, failure to maintain the system's security level over time will lead to a degradation which might undermine any previous hardening that has been performed.

It is therefore recommended that systems be subjected to regular reviews designed to identify:

- Missing patches
- Changes to the initial configuration as a result of software installation
- Insecure use cases which might result in passwords or other sensitive information being disclosed
- Further changes that can be made to the configuration, considering recognized improvements in security best practices

### **Configure Systems In-line With Industry Best Practices**

Poor configuration control could enable an attacker to obtain a foothold within the network or environment. Poor configuration includes the retaining of vendor-supplied default settings and passwords, which can often be easily guessed, and services being enabled unnecessarily.

All systems within the IT environment should be reviewed and their configurations brought into line with security industry best practices. In addition, strict change control should be applied with regards to all production systems.

### **Implement File Upload Restrictions**

Ensure that web application file upload functionality is implemented according to security industry best practice guidelines.

### **Implement A Robust Approach To Password Management**

Strict rules governing the setting of passwords should be created and a policy implemented that enforces the use of strong and complex values, as per the recommendations contained within this report. It is important that passwords are not reused across accounts on the same systems, or across multiple servers, to lessen the likelihood of a higher number of individual systems or components being compromised.

## 2. Project Summary

Members of the Cisco Advisory team have served as trusted business advisors, cyber security leaders, and technical experts in a wide range of roles. Together we use our vast experience in cyber security, risk management, and technical innovation to help our clients across every industry advance their business objectives.

### 2.1 Project Scope

Cisco performed a remote penetration test of Exemplum's externally facing network environment supporting the e-commerce business unit. The following ranges of hosts were considered in-scope for this engagement:

- [REDACTED]
- [REDACTED]
- [REDACTED]

### 2.2 Project Teams

Cisco Project Team		
Team Member	Project Role	Contact Information
Alice Andrews	Team Lead	aandrews@cisco.com
Bob Brown	Project Manager	bbrown@cisco.com

Exemplum Project Team		
Team Member	Project Role	Contact Information
Christine Cooper	Executive Sponsor	ccooper@exemplum.com
David Douglas	Project Manager	ddouglas@exemplum.com

## 3. Technical Analysis

---

### 3.1 Technical Summary

At the request of Exemplum, Cisco performed an External Network Penetration Test of Exemplum's external Internet presence. A penetration test is a type of "ethical hacking" or "intrusion testing" approach for detecting computer system vulnerabilities that malicious intruders could use to exploit a system and compromise its data. The assessment took place between December 12 and 16, 2022.

The primary objective of the engagement was to determine whether an external attacker could compromise Exemplum's systems or data. In addition to typical engagement objectives, Exemplum requested that Cisco place particular emphasis on compromising the quoting and ordering system. Using a combination of vulnerabilities, Cisco successfully gained access to client and order data, proprietary manufacturing specifications, internal communications, and the Exemplum VOIP (telecommunications) system.

Overall, Cisco identified eight (8) findings, including one (1) Critical, two (2) High, two (2) Medium, two (2) Low, and one (1) informational finding.

#### **Initial Reconnaissance & Foothold**

Using network scanning and publicly available intelligence sources, several interesting targets were identified. These included a misconfigured VOIP server, an out-of-date SSH server, a WebDAV file share, and custom sales functionality on the clientx.com website.

The WebDAV share at support.clientx.com does not require identification or authentication. Anonymous access to the share revealed sensitive data related to customer support requests, including email addresses, usernames, and temporary passwords. Cisco tested a sample of temporary passwords and found one to still be valid, granting access to Exemplum's account on clientx.com.

The compromised customer account granted access to the customer-restricted section of the Exemplum website, which contained a file upload vulnerability. Cisco exploited this vulnerability by uploading a web shell to gain remote command execution on the application server.

During the engagement, Cisco performed targeted remote password guessing attacks, which were successful on multiple systems. Using the access available on these systems, Cisco was able to obtain a significant amount of sensitive data, including customer prototype specifications, contracts, and work orders. One of the compromised servers was the VOIP management server, which controls phone and voicemail functionality. After discussing the risks associated with modifying the VOIP server configuration with the Exemplum Technical Point of Contact, a decision was made to refrain from making any configuration changes that could have led to additional compromises. The VOIP server also exposed a VxWorks console (Finding 5) which effectively grants the same level of access.

### Further Compromise and Pivot

Using the access gained from exploiting a file upload vulnerability, Cisco enumerated application configuration files related to the file store at cloud.clientx.com. A temporary file stored in the application working directory contained the API key being used to manage data at cloud.clientx.com. This key granted full read and write access to customer order data and customer technical specifications.

While investigating the compromised SSH service, Cisco found a user's shell history file which contained an instance of a "mount" command being used to mount a remote filesystem. This instance also recorded the password to access the remote system. Cisco used the password to remount and access the remote filesystem. The shared drive contained a copy of the contents of the corporate Intranet website, allowing Cisco to access internal-only employee communication records and files.

### Other Findings

In addition to the major vulnerabilities present in the environment, Cisco also observed several sensitive services which should generally not be exposed to the Internet. Finally, Cisco identified several hosts using weak or deprecated SSL/TLS configurations for transmission of sensitive data.

## 3.2 Summary of Findings

### STRENGTHS

Exemplum network-based access control devices and host-based firewall software enforced strong controls in order to restrict inbound connections to sensitive services such as Microsoft Terminal Services and Microsoft SQL Server.

Exemplum developers implemented strong validation of user-supplied input in order to prevent SQL injection (SQLi), cross-site scripting (XSS), and other common classes of web application attacks.

### WEAKNESSES

#### Inadequate Password Policy

##### DESCRIPTION

Allowing weak or predictable passwords to be used, or passwords to be reused across systems, leads to a greater likelihood of systems being compromised.

##### SOLUTION

Cisco recommends that a robust approach is taken to password use within an organization. Passwords should have an appropriate complexity based on the type and level of access and the systems on which they can be used. Each password should be created from a large character set that forces the user to select a combination of uppercase, lowercase, numbers, and special characters. In addition, passwords should not be based on a dictionary word, the username, or the associated system.

#### Insecure Access Control Mechanism

##### DESCRIPTION

The software does not restrict, or incorrectly restricts, unauthorized access to a resource.

#### SOLUTION

Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn, and prohibit sensitive data from travelling outside of these boundaries, especially when interfacing with a system outside of the safe area. The appropriate compartmentalization should be built into the system design to allow for further reinforcing of privilege separation. Architects and designers should always follow the principle of least privilege.

### **Insecure Configuration**

#### DESCRIPTION

Insecure configuration can lead to sensitive information being disclosed or services being exposed to attack.

#### SOLUTION

Modify the current configuration files to ensure they adhere to security industry best practices, and conduct regular configuration reviews to ensure that current variables are up-to-date.

### **Insufficient Access Controls**

#### DESCRIPTION

Access controls are not implemented properly, allowing users to access functionality outside of their intended remits.

#### SOLUTION

Ensure access control lists are correctly implemented to ensure that pages intended to be accessed only at certain points in the application workflow are properly segregated.

### **Leftover Debug Code**

#### DESCRIPTION

The application contains debugging code that can expose sensitive information to untrusted parties.

#### SOLUTION

Do not leave debug statements that could be executed in the source code. Assure that all debug information is eradicated before releasing the software.

## Unrestricted Upload of Dangerous File Types

### DESCRIPTION

It would be possible for an attacker or malicious user to upload or transfer dangerous file types that could be automatically processed within the environment.

### SOLUTION

It should be assumed that all user-supplied input is malicious and, therefore, strong input validation mechanisms should be in place. An allowlist of acceptable inputs that strictly conform to specifications and that rejects any input that does not strictly conform (or transforms it into an acceptable type) should be considered. Input validation should include all potentially relevant properties including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields and conformance to business rules. It is not sufficient to simply detect malicious or malformed inputs (i.e., a denylist) as undesirable inputs may not be fully accounted for, especially if the code's environment changes, hence providing room for an attacker bypassing the intended validation. Denylists can, however, be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright; for example, limiting filenames to alphanumeric characters can help to restrict the introduction of unintended file extensions.

**INDEX OF FINDINGS**

Finding Title	Severity Rating	CVSS Score
1. Insecure File Upload	<b>CRITICAL</b>	<b>9.1</b>
2. Default & Weak Passwords	<b>HIGH</b>	<b>8.9</b>
3. WebDAV Anonymous Read & Write	<b>HIGH</b>	<b>8.7</b>
4. Unprotected Memcached Instance	<b>MEDIUM</b>	<b>6.6</b>
5. VxWorks WDB Debug Service Present	<b>MEDIUM</b>	<b>5.3</b>
6. Insecure Credential Management Practices	<b>LOW</b>	<b>3.7</b>
7. Insecure SSL/TLS Configuration	<b>LOW</b>	<b>3.0</b>
8. Robots.txt File	<b>NONE</b>	<b>0.0</b>



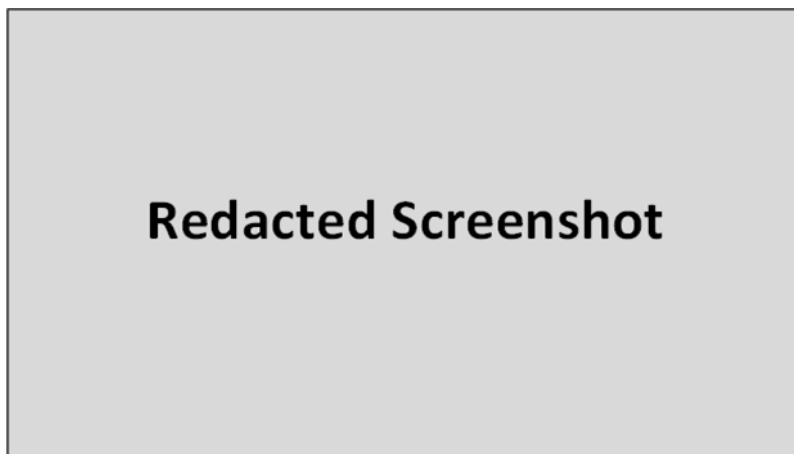
## 4. Detailed Findings

1. Insecure File Upload			
Severity Rating	CRITICAL	CVSS Score	9.1
CWE Category	CWE-434: Unrestricted Upload of Dangerous File Types		
Affected Components	[REDACTED]		

### Specific Detail

Cisco found that the "Get A Quote" data upload feature of the public production and QA websites did not correctly restrict the content and name of uploaded files. Furthermore, it writes the uploaded file contents using the provided name to a directory that the web server provides remote access to via HTTPS.

By uploading a malicious ASP file to the vulnerable servers and using the "preview" feature, a remote unauthenticated attacker can run operating system commands and execute arbitrary code on the system as the "Network Service" user.



*Figure 1 - Remote shell access to the server*

The web shell backdoor providing command execution that was uploaded during exploitation was named [REDACTED] and was deleted after post-exploitation activities were complete.

### Vulnerable URLs

████████████████████

████████████████████

### General Background

Insecure file upload vulnerabilities occur when an application names an uploaded file based on a value derived from user input. This condition can be exploited to elevate privileges within the application or deny service to users by overwriting files on the server.

File upload vulnerabilities also result when users can specify the extension of the file on disk. This condition can be exploited to run arbitrary code by assigning an uploaded file an extension used to identify scripts (e.g., PHP, ASP, and JSP). If the uploaded file is subsequently accessed by URL, the active scripting platform might interpret the file and execute its contents, allowing an attacker to execute unauthorized operations on the application server.

### Impact

Insecure file upload vulnerabilities can be exploited to execute arbitrary code, elevate privileges within the application or deny service to users. In this case, code execution occurs as the Network Service system user.

As a proof of concept, Cisco uploaded an ASP web shell which granted interactive access to a Windows command shell on the server. With this access, Cisco was able to view detailed information from Exemplum customers, including sensitive intellectual property, internal pricing information, and vendor guidance documents.

Cisco used this access to examine configuration files used by the "Get A Quote" feature. One file revealed a session key used to manage data in customer directories on ██████████. Cisco used this key to remotely access the API of ██████████ and read further customer data.

### Recommendation

Cisco recommends that Exemplum limit the file types that can be uploaded, in particular, limiting any executable files, such as EXE, ASP, PHP, and JSP. These type checks should be implemented against the file extension and the file format. If file format verification is used, ensure the file format identification library is kept up-to-date as these are known to contain vulnerabilities.

Ensure users cannot control the destination path or extension of an uploaded file. The destination directory as well as the file extension should both be chosen by the server. If possible, user input should be rejected if it does not validate against an allowlist of acceptable input (e.g., only alphanumeric).

Also, consider storing the data inside the database. If it must be stored on the file system, do not store the file under the web server document root and have the application enforce access control to the file. If possible, do not use user input to derive a filename for storage; instead, generate a GUID to store and reference the uploaded file. Ensure that existing files are not overwritten.

Consider performing antivirus scanning on uploaded files as an additional layer of defense. Ensure the antivirus software is kept up-to-date as these have been known to contain vulnerabilities that malicious file uploads can exploit.

The backdoor upload and use were not detected during the testing. Ensure any network-based intrusion detection systems have sensors that can see decrypted HTTP traffic (i.e., the sensors are placed after HTTP reverse proxies and load balancers have decrypted the HTTPS stream).

Host-based intrusion prevention and detection systems typically contain functionality that can detect commonly used web backdoors and unsophisticated post-exploitation behavior, but sophisticated attackers that build their own tools can usually evade such detection.

2. Default & Weak Passwords			
Severity Rating	<b>HIGH</b>	CVSS Score	<b>8.9</b>
CWE Category	CWE-0: Inadequate Password Policy		
Affected Components	<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px;"></div>		

### Specific Detail

Through password guessing, Cisco was able to obtain administrator/root level access to two components of the VOIP system, root access on an SSH server, and "author" level access to the marketing blog.

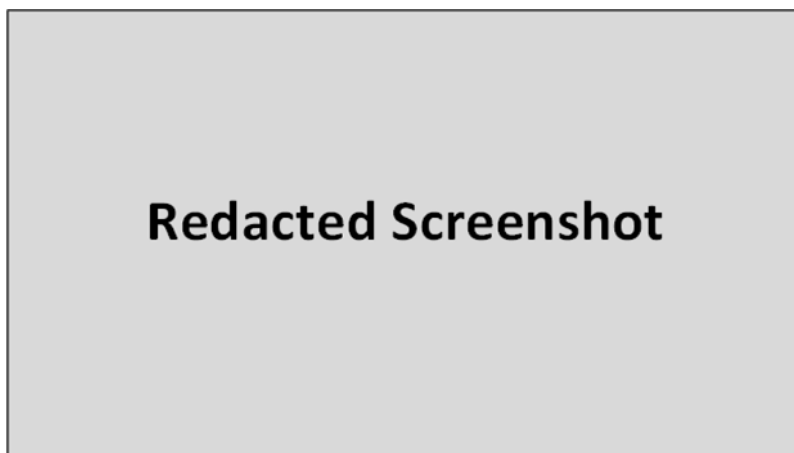


Figure 2 - A password guessing tool using a list of network hardware default passwords has identified valid credentials for the service at [REDACTED]

Service	Username	Password
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

### Impact

With administrative access to the VOIP system, an attacker could redirect voice traffic to a system under their control, arbitrarily add new telephony devices to the system, or take the system offline entirely. Cisco did not make changes to the VOIP system but confirmed access to those functions and examined system logs and the system configurations of these devices.

With "author" access to the marketing blog, an attacker could post new content or edit existing content, potentially damaging Exemplum's brand or reputation. Cisco confirmed this level of access by making a small invisible change to an existing post, then reverting that change after confirmation.

Finally, the remotely accessible "root" account on the [REDACTED] server used a weak password which could be inferred from content on the Exemplum website. After accessing this account, Cisco found database credentials in a user's history file.

### Recommendation

Cisco recommends that default passwords should be reset immediately to a value compliant with a strong password policy. Additionally, future deployment or application and system accounts should use passwords that are randomly generated and follow require compliance with a strong password policy. System build procedures should be updated to require this practice.

Review application and account activity to determine whether an account with a default password was used without authorization. If possible, determine the extent of such usage and likelihood of further compromise.

Consider the use of a password manager to help users manage unique, strong passwords across multiple systems. Also consider the use of two-factor authentication (2FA) on particularly sensitive systems.

3. WebDAV Anonymous Read & Write			
Severity Rating	HIGH	CVSS Score	8.7
CWE Category	CWE-0: Insecure Access Control Mechanism		
Affected Components	[REDACTED]		

### Specific Detail

Two of the systems in scope for this assessment were running WebDAV. One system, [REDACTED], allows unauthenticated access to WebDAV, exposing internal and sensitive information present on the file system.

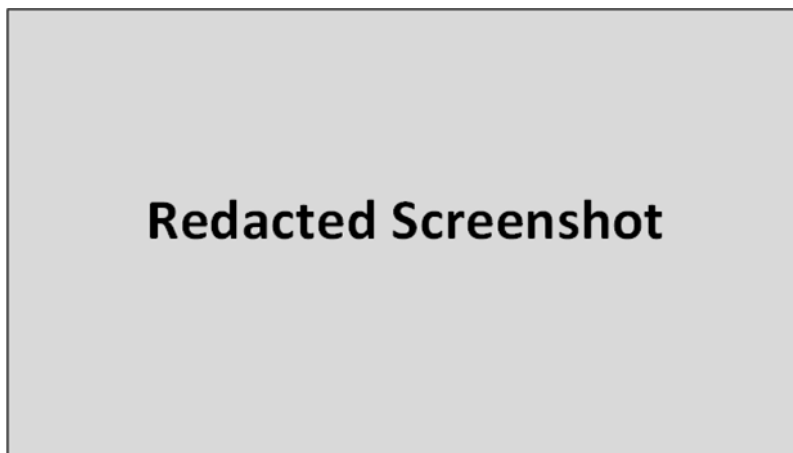


Figure 3 - Sample of sensitive files present on WebDAV server

### General Background

WebDAV is a set of HTTP methods that allows for collaborative file editing, similar to file shares or FTP. Anonymous access does not require any identification or authentication and provides immediate access to any data available to the "anonymous" role.

### Impact

Cisco was able to access sensitive files on the system that supports unauthenticated access. This includes contracts, work orders, emails, and other internal and sensitive information. Cisco also validated that files can be uploaded using WebDAV, potentially allowing an attacker to use this vulnerable system as their own personal file server.

Attackers may use the file server to conduct "watering hole" or phishing attacks against server users. These types of attacks exploit user trust in the system to compromise each user that accesses the server.

If users are currently using this access for legitimate duties, there is a loss of accountability. A user might access or delete a file and it might be impossible or difficult to prove that the user actually accessed or deleted the file because their username was not recorded.

### Recommendation

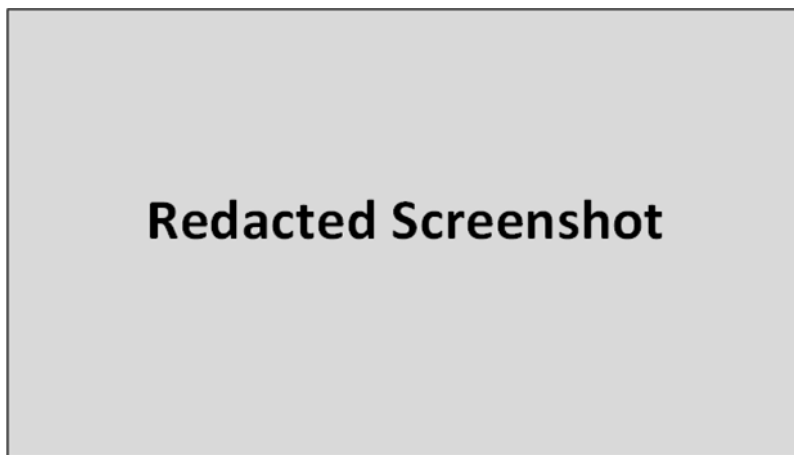
Disable the HTTP PUT and DELETE methods if file upload and delete functionality is not needed. If WebDAV is not used, disable it entirely. If it is necessary, disable unauthenticated access and require per-user authentication. Consider implementing an additional layer of protection and restrict access to these servers from the public Internet via a firewall or other network-layer device.

Review the currently accessible data and type of data that might have been accessible at this location in the past. For sensitive data, review access logs and attempt to identify unauthorized access attempts. Ensure the accessed data does not contain sensitive information about third parties, customers, or individual PII. If it does, consider notifying the affected organizational or individuals of the potential breach.

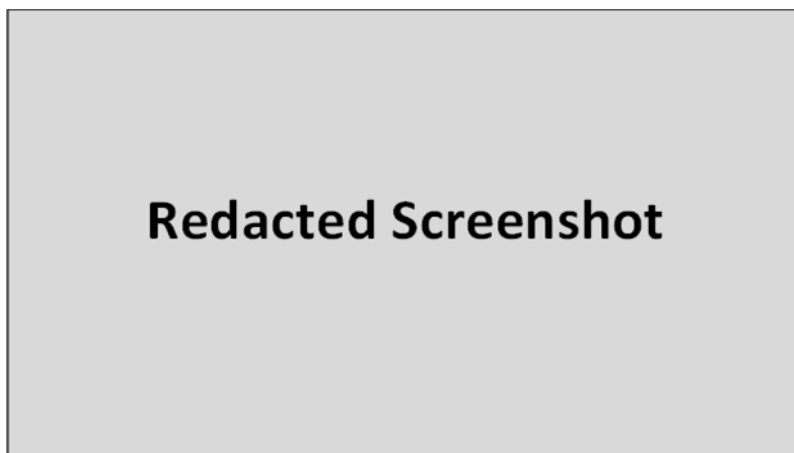
4. Unprotected Memcached Instance			
Severity Rating	MEDIUM	CVSS Score	6.6
CWE Category	CWE-284: Insufficient Access Controls		
Affected Components	[REDACTED]		

### Specific Detail

Cisco identified an exposed Memcached service without any authentication or access control.

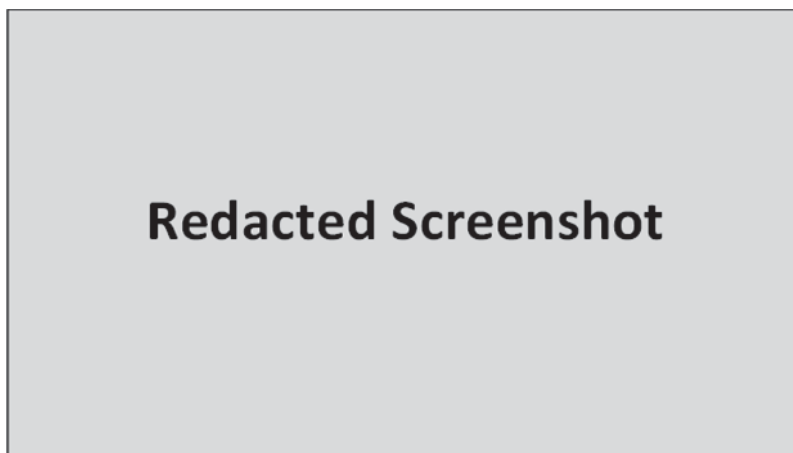


*Figure 4 - A partial list of cached records. The "config" files are visible in this cache slab and can be accessed with a further request.*



*Figure 5 - Reading a configuration file; this file contains hundreds of keys, only a few are shown*





*Figure 6 - Demonstrating write-access to Memcached*

### General Background

Memcached is a high-performance key-value store used to enhance the performance of other applications. As it is optimized for speed, Memcached incorporates no security mechanisms and must be protected via network isolation.

### Impact

As Memcached does not incorporate any security of its own, an attacker able to connect to the service can read and write all keys or destroy all cached data to create a denial-of-service.

Services that rely on data from Memcached might function differently or allow injection of malicious content (such as HTML, CSS, or JavaScript) which could be used to conduct further attacks, such as cross-site scripting, on application users.

As a proof of concept, Cisco identified and accessed keys which appeared to contain sensitive configuration information, including:

- cx\_smtp\_addr
- cx\_smtp\_usr
- cx\_smtp\_pass
- cx\_passreset\_hmac\_key

In discussion with Exemplum personnel, Cisco confirmed that these values are used by the password reset and notification functionality in the property management application. An attacker tampering with these values could arrange to receive password reset emails for any user, allowing full takeover of the account.

Cisco also demonstrated the ability to create, delete, and modify keys using a new key [REDACTED]. Out of concern for Exemplum's production network stability, Cisco did not attempt to tamper with any existing keys.

**Recommendation**

Cisco recommends isolating all instances of Memcached using a proper architecture that places Memcached “behind” the application. Firewalls, VPNs, and strict network access control lists can also be used to provide this isolation. Only services with a legitimate business need should have access to a Memcached service.

5. VxWorks WDB Debug Service Present			
Severity Rating	MEDIUM	CVSS Score	5.3
CWE Category	CWE-489: Leftover Debug Code		
Affected Components	[REDACTED]		

### Specific Detail

Cisco discovered a device with a VxWorks WDB Debugging Agent running. A vulnerability in this service allows for remote read and write of the system memory, potentially leading to a complete compromise of the device.

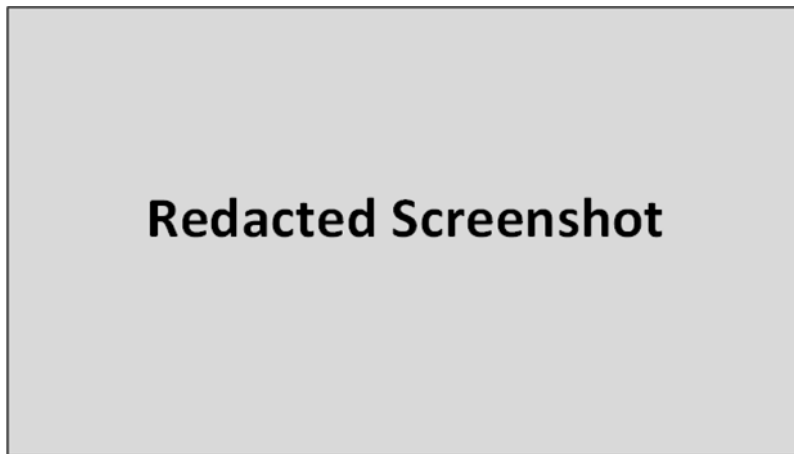


Figure 7 - Remote memory disclosure on the PBX device

### General Background

VxWorks is a real-time operating system. The WDB component is intended as a development and debugging aid and should not be exposed to untrusted networks, but it is installed by default. Please refer to the following resource for more information regarding this vulnerability:

<https://www.kb.cert.org/vuls/id/362332>

### Impact

The vulnerable device is a VOIP PBX. Access to the system memory could provide an attacker with sensitive information about the configuration of the system. Additionally, it could allow an attacker to overwrite running system memory, leading to a denial-of-service condition.

Cisco was able to dump system memory and obtain encrypted remote access credentials. The encrypted credentials were cracked using an offline dictionary password guessing attack.

#### **Recommendation**

Cisco recommends disabling the debugging service or contacting the system vendor for a patch. In general, configure firewall rules to allow inbound access only to ports specifically needed for legitimate use.

6. Insecure Credential Management Practices			
Severity Rating	LOW	CVSS Score	3.7
CWE Category	CWE-522: Insufficiently Protected Credentials		
Affected Components	██████████		

### Specific Detail

After gaining access to an SSH server, Cisco found systemic mishandling of user and system credentials.

These practices included:

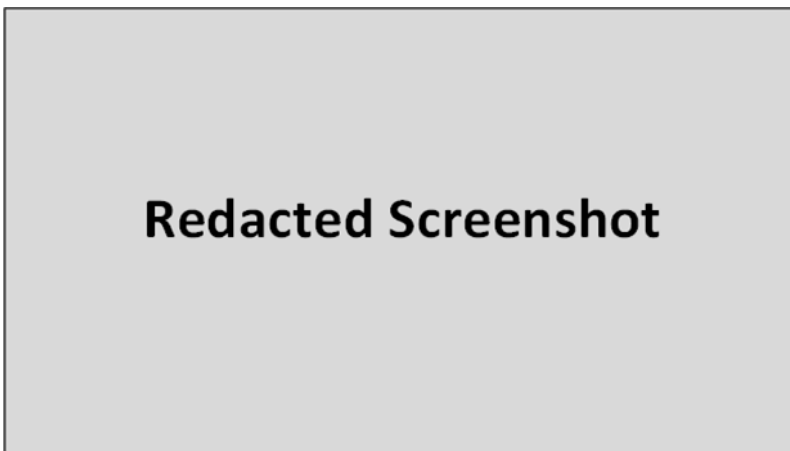
- Plaintext passwords on the command line
- Plaintext storage of credentials in various utility scripts and cron jobs
- Unencrypted "passwords.txt" and "credentials.yaml" files in user and service directories
- Excessively permissive file permissions

#### Plaintext Passwords on the Command Line

Cisco was able to mount a file share used to back up the Exemplum intranet website because command-line logging is enabled, and a user had insecurely specified a password on the command-line. The ██████████ user had issued the ██████████ command to remotely mount the filesystem of the ██████████ server. This user had insecurely specified the password in plaintext on the command-line instead of letting the mount command prompt the user to input the password. The password was recorded to the user's history file where it was found and reused to gain unauthorized access to intranet data. Cisco found three instances of users issuing the mount command in this insecure manner.

#### Plaintext Storage of Credentials in Utility Scripts

Cisco identified several copies of utility scripts which contained hard coded user and system credentials. Documentation in several of the scripts identified them as part of a "ServerUtils" repository maintained by the Operations team. Many of these template scripts had variables intended for users to hardcode their credentials. These hardcoded credentials gave access to four valid username and password pairs.



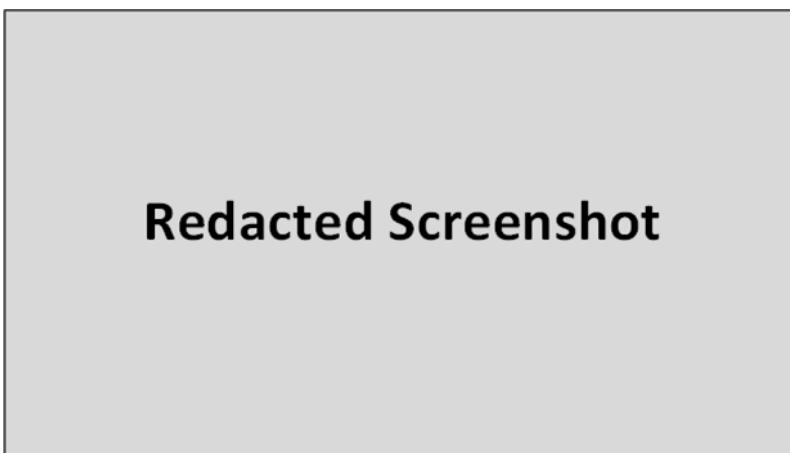
*Figure 8 - Cleartext credentials in a utility script*

#### **Plaintext "password.txt" and "credentials.yaml" Files**

To streamline management of service and database passwords, several users kept cleartext copies of these credentials in configuration files. Like the hardcoded utility scripts, these files allowed Cisco to quickly harvest valid credentials using simple filesystem searching commands.

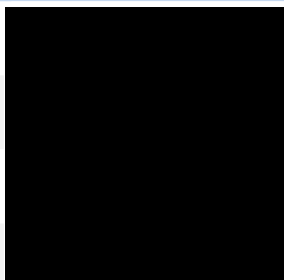
#### **Excessively Permissive File Permissions**

Multiple user home directories and files containing credentials did not have sufficiently restrictive access controls. Two user accounts had ".history" files world readable, and three user accounts had either "passwords.txt" or "credentials.yaml" readable by all system users.

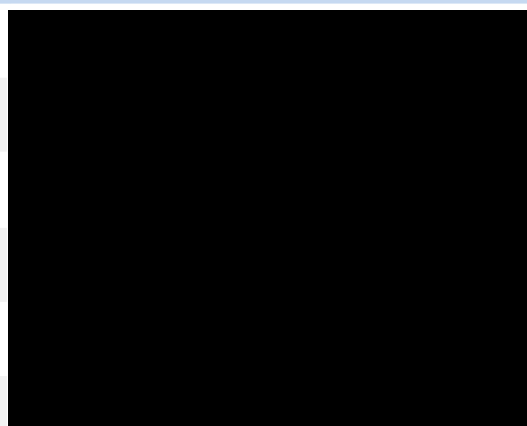


*Figure 9 - Permissions and contents of a .history file contain a password to another system*

### World Readable Home Directories



### Accessible Files Containing Plaintext Passwords



### General Background

Systems commonly support secure and insecure modes of operation. The security of these systems is dependent upon which mode the application user chooses to invoke. Simply disabling support for the insecure mode of operation is often insufficient to fully resolve security concerns with these systems. User education is required to help avoid attempts at insecure system use.

### Impact

Disclosure of credentials may lead to other systems being compromised. Cisco was able to use the credentials to obtain a complete copy of the Exemplum intranet site.

Low-privileged users can access sensitive files since operating system enforced access controls are not used to protect the files. Even if the files are encrypted, low-privileged users can attempt to decrypt the files.

### Recommendation

Cisco recommends educating system users to use applications in a secure manner. Specifically, they should never type passwords into systems that do not obscure password entry and they should only provide their passwords when prompted to do so by the system.





7. Insecure SSL/TLS Configuration			
Severity Rating	LOW	CVSS Score	3.0
CWE Category	CWE-326: Inadequate Encryption Strength		
Affected Components	[REDACTED]		

### Specific Detail

Cisco observed, but did not exploit, several issues with Exemplum’s transport security configuration.

#### Protocol Vulnerabilities

- SSLv2, SSLv3, and TLSv1.0 are in use
- The PCI standards council no longer considers SSLv2.0, SSLv3.0, TLSv1.0, or TLSv1.1 to be strong cryptography, and these can no longer be used
- SSLv2 has a known server authenticity vulnerability and has been deprecated since 1996
- SSLv3 is vulnerable to the Padding Oracle On Downgraded Legacy Encryption (POODLE) flaw, which allows an attacker to decrypt one plain text bit in as few as 256 tries
- TLSv1.0 is vulnerable to the Browser Exploit Against SSL/TLS (BEAST) attack, which can be used along with a flaw in CBC ciphers to encryption through a victim’s web browser
- TLSv1.1 does not support several strong ciphers

#### Cipher Suite Vulnerabilities

- Medium strength ciphers in use: EDH-RSA-DES-CBC-SHA, DES-CBC-SHA
- Weak strength ciphers in use: EXP-EDH-RSA-DES-CBC-SHA, EXP-DES-CBC-SHA, EXP-RC2-CBC-MD5, EXP-RC4-MD5
- RC4 and DES-CBC3 ciphers have weaknesses that allow attackers to recover the plain text of a session

#### Certificate Vulnerabilities

- SHA1 with RSA is used to sign a certificate. This algorithm is considered insecure and has been deprecated by modern systems
- Self-signed certificates
- Expired certificates

Many of these vulnerabilities are rarely exploited in the wild and much of the risk relates to compliance considerations. Exploitation of these vulnerabilities is usually not necessary for attackers, since users frequently accept invalid certificates. Legitimate systems with certificate vulnerabilities promote the user behavior that attackers take advantage of.

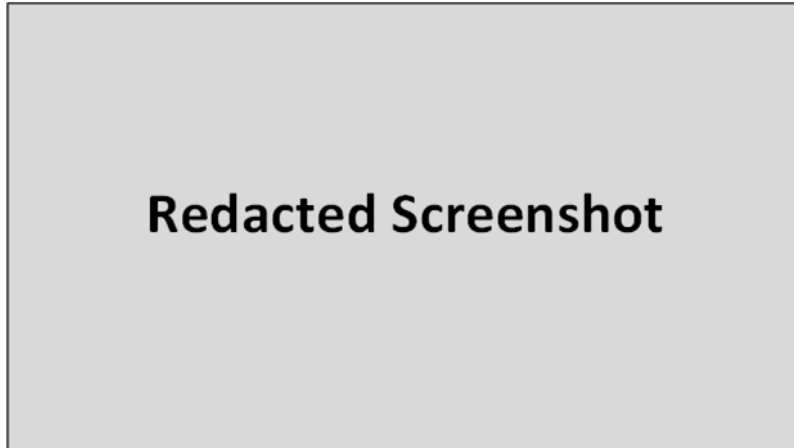


Figure 10 - The "sslyze" tool is used to identify insecure SSL/TLS configuration

### General Background

Cryptographic technologies derive their security from an assumed high degree of effort needed to compromise them. Protocols in active use, including SSL and TLS and their options, as well as ciphers are subject to constant vulnerability research that can be academic or malicious in nature. When a protocol or cipher weakness is identified that is either practically exploitable or signals an advance in the state of the art of research, the industry actively discontinues its use. An application that continues to use weak cryptographic protocols, options, and ciphers increases its chances of compromise.

### Impact

Use of weak or compromised protocols, protocol options, or ciphers increases the chances that an application's data, including administrator or user credentials, personally identifiable information, protected cardholder data, or monetary transactions may be compromised.

### Recommendation

Cisco recommends configuring servers in a consistent manner to:

- Disable SSLv2, SSLv3, TLSv1.0, and TLSv1.1
- Disable medium and weak strength ciphers
- Disallow client-initiated renegotiations
- Use the TLSv1.2 and TLSv1.3 protocols
- Prefer the ECDHE-RSA-AES256-SHA and ECDHE-RSA-AES128-SHA ciphers and the AES-GCM family of ciphers
- Use SHA256 when updating digital certificates

Avoid self-signed certificates but if they are needed ensure every client has the signer's certificate in their trusted certificate store.

Establish a process to renew certificates prior to expiration.

Test the new configuration before deployment to production to ensure legitimate clients can continue to access the system.

8. Robots.txt File			
Severity Rating	NONE	CVSS Score	0.0
CWE Category	CWE-200: Information Exposure		
Affected Components	[REDACTED]		

### Specific Detail

The "robots.txt" file was deployed on the web server in order to prevent search engine robots from indexing certain files and directories.

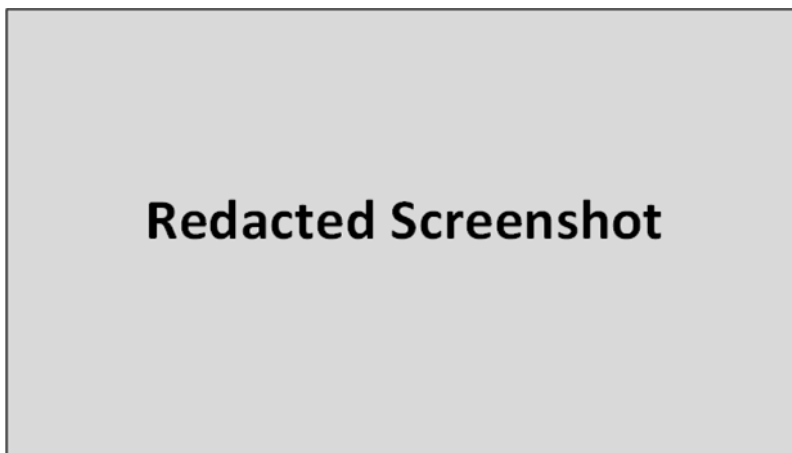


Figure 11 - The robots.txt file lists specific web application pages

### General Background

The "robots.txt" file prevents search engine robots from indexing certain files and directories. However, the "robots.txt" file could inadvertently disclose sensitive information.

### Impact

Depending on the information contained within the "robots.txt" file, attackers could identify the location of sensitive files and directories.

In this case, overly sensitive information was not identified within the "robots.txt" file. However, this finding is included as specific web application pages were listed within the "robots.txt" file.

### Recommendation

Cisco recommends not deploying the "robots.txt" file. Instead, include the following "META" tag on every page that search engine robots should ignore:

```
<meta name="robots" content="noindex, nofollow">
```

The "noindex" value instructs robots not to index content within the page, and the "NOFOLLOW" value instructs robots not to follow links within the page.

## Appendices

### Appendix A: CVSS Vector Strings

**1. Insecure File Upload**

[AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/RC:U](#)

**2. Default & Weak Passwords**

[AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/RL:W/RC:C](#)

**3. WebDAV Anonymous Read & Write**

[AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:H/RL:O/RC:C](#)

**4. Unprotected Memcached Instance**

[AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:F/RL:W/RC:C/CR:L/IR:L](#)

**5. VxWorks WDB Debug Service Present**

[AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

**6. Insecure Credential Management Practices**

[AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

**7. Insecure SSL/TLS Configuration**

[AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/CR:L/IR:L](#)

**8. Robots.txt File**

[AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N](#)

## Appendix B: Definition of Terms

Each finding identified during the assessment is allocated a Severity Level and CVSS 3.0 score. The Severity Level was directly derived from the CVSS 3.0 score as per the standard, as well as being described under the Specific Details, Security Impact, and Recommendations headings, with an additional Reproduction Steps header where applicable. The ratings are based on the individual objective finding and not the subjective risk the issue may pose.

### COMMON VULNERABILITY SCORING SYSTEM (CVSS)

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three (3) groups: Base, Temporal, and Environmental.

Each group produces a numeric score ranging from 0 to 10, and a Vector, which is a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

Cisco uses the CVSS 3.0 scoring mechanism and directly maps those to severity ratings for each finding, as defined in the CVSS 3.0 standard shown below:

Severity Rating	CVSS Score
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
None	0.0

## COMMON WEAKNESS ENUMERATION (CWE)

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code
- Serve as a standard measuring stick for software security tools targeting these weaknesses
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts

Cisco applies a relevant CWE against each finding in order to allow for finding grouping, which is then used to generate the remediation action plan in the recommendations section of the report.





---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



# Cisco Security Services



Test Company

Web Application Assessment

April 06, 2018

**Technical Report**

**Draft**

## About This Document

Document Information	
<b>Author</b>	sdtrych
<b>Change Authority</b>	Cisco Systems Advanced Services
<b>DCP Reference</b>	000000
<b>Project ID</b>	000000
<b>Task Reference</b>	000000SAQ

Document History			
Version	Date	Status	Comments
0.1	06/04/2018	Draft	1st Draft Technical Report - Cisco

Document Review		
Reviewer	Version	Date

This document contains and constitutes the proprietary and confidential information of Cisco ("Cisco"). It is provided to Test Company ("Company") subject to and in accordance with the terms of any agreement between Cisco and the Company regarding treatment of confidential information and/or licensing of proprietary information. This document also contains information that is highly sensitive confidential information of the Company and should be treated by representatives of the Company accordingly. This document may not be distributed by the recipient without the express permission of Cisco and the Company.

The contents of this document do not constitute legal advice. Cisco's offer of services or deliverables that relate to compliance, litigation, or other legal interests is not intended as legal counsel and should not be taken as such.

# Table of Contents

- Table of Contents ..... 4
- 1. Executive Summary ..... 6
  - 1.1 Introduction..... 6
  - 1.2 Conclusions..... 6
  - 1.3 Recommendations..... 7
  - RECOMMENDED ACTION PLAN..... 7
- 2. Project Summary ..... 9
  - 2.1 Project Scope ..... 9
  - 2.2 Project Teams ..... 9
- 3. Technical Analysis..... 10
  - 3.1 Technical Summary..... 10
  - 3.2 Summary of Findings ..... 11
    - STRENGTHS ..... 11
    - WEAKNESSES..... 11
    - INDEX OF FINDINGS..... 13
- 4. Web Application Assessment..... 14
- Appendices ..... 36
  - Appendix B: General SSL Recommendations..... 37
    - APPENDIX B.1: SAMPLE IMPLEMENTATIONS ..... 37
      - APACHE ..... 37
      - IIS ..... 37
    - APPENDIX B.2: RECOMMENDATIONS..... 38
      - CIPHER SUITES ..... 38
      - CONFIGURATION..... 38
      - CERTIFICATES ..... 38
      - CLIENTS..... 38
  - Appendix C: Generic Assessment Methodology ..... 39
    - FOR EACH SERVICE PERFORMED IN SUPPORT OF THIS REPORT, INCLUDE A SINGLE PAGE METHODOLOGY IN THE APPENDIX: ..... 39
    - IN GENERAL, IT SHOULD INCLUDE THE FOLLOWING ..... 39
    - ONCE WRITTEN, ENSURE YOUR NEW METHODOLOGY IS INCLUDED IN GITLAB SO THAT IT CAN BE ROLLED BACK INTO XDB ..... 39
    - ONCE PEER REVIEW IS COMPLETE, PLEASE UPDATE THE XDB TASK WITH CHANGES MADE DURING THE PEER REVIEW TO ENSURE THAT THE INFORMATION IN XDB IS UP TO DATE WITH THE DELIVERABLE THAT WAS PROVIDED TO THE CLIENT..... 39
  - Appendix D: Definition of Terms ..... 40
    - CVSS..... 40
    - CWE ..... 40



# 1. Executive Summary

---

## 1.1 Introduction

Cisco was asked by Test Company to perform a security assessment of their internet-based 'Concrete2.0' web application, used by employees as a social network to interact with each other. The application also has a 'News' section that is publicly accessible and 'Document Portal' that can be used to make documents publicly accessible.

The application has recently been upgraded from Concrete1.0. Test Company therefore engaged Cisco to gain greater visibility of any security risks that may have been introduced during the upgrade. Testing was carried out on a pre-production environment prior to 'Concrete2.0' being deployed on the internet-facing production environment. Consideration was given to attack against the application from an unauthenticated point of view and from the point of view of attackers with normal user credentials.

Some of the 'Concrete2.0' features like 'News' or 'Document Portal' were freely accessible by anyone. However, to comment articles and view status updates, employees need to log in. Two different roles were available in the web application: ██████ and '█████'.

The main aims of this assessment were to determine whether the individual elements making up the solution were configured in line with current industry good security practice guidelines and, specifically, to provide answers to the following pre-determined questions:

- Did the web application exhibit any flaws or vulnerabilities that could enable an attacker to compromise the confidentiality, integrity, or availability of the data stored?
- Had sufficient security hardening measures been carried out to reduce the attack surface of the web application?
- Were communications within the web application suitably protected from interception and general intervention?

Test Company were particularly keen to gain assurance that the 'Concrete2.0' prevents users from accessing each other's accounts and escalating their privileges to admin level.

During testing, the Team also looked to identify and report any measures that could improve security and strength in depth within the application under assessment.

Testing was conducted between the 22<sup>nd</sup> and 25<sup>th</sup> of November 2016 from the Cisco premises in Hertfordshire, UK. Testing was conducted as stipulated in the Terms of Reference and no problems were encountered.

## 1.2 Conclusions

The assessment identified several High severity security issues in the instance of 'Concrete2.0' running in the pre-production User Acceptance Testing (UAT) environment. The assessment team notified Test Company of each High severity security issue during the course of the assessment to provide early visibility and an opportunity to fix the vulnerabilities identified.

If the 'Concrete2.0' web application were to be deployed to the live environment without being fixed, the security issues identified would be sufficiently serious to pose a risk of reputational damage to Test Company or incur significant financial costs to clean up after a breach:

- The website could be defaced and used to host illegal content
- Data could be stolen from the site and used in other attacks on Test Company - e.g. employee names, usernames and passwords.

In order to respond as directly as possible to the questions posed at the outset of this engagement, the questions from the previous section have been duplicated below and the assessment team have responded to each:

**Did the web application exhibit any flaws or vulnerabilities that could enable an attacker to compromise the confidentiality, integrity, or availability of the data stored?**

High severity vulnerabilities that could impact the confidentiality integrity, and availability of the web application were present. These are summarised below and detailed in the body of the report, along with recommendations on how to fix vulnerabilities and reduce risk.

### **Had sufficient security hardening measures been carried out to reduce the attack surface of the web application?**

Additional controls and mechanisms should be implemented to harden the web application.

### **Were communications within the web application suitably protected from interception and general intervention?**

The website had been configured to use SSL encryption to protect connections to the website from eavesdropping and tampering. SSL security was reviewed and found to be in line with good security practice, providing a good level of protection when used.

However, the the site was also accessible without SSL. Even though users would normally be redirected to the SSL-protected site, user traffic could still be at risk of of eavesdropping and modification. The Technical Summary section goes into more detail and the body of the report provides detailed recommendations that can be implemented easily to improve the security of website traffic.

### **Did the web application prevent users from accessing each other's accounts and escalating their privileges to admin level?**

The application implemented a robust approach to privilege handling by employing session management that was in line with good security practices and per-page access control lists that prevent unauthorised access to administration features.

However, some of the other serious vulnerabilities identified did provide ways for attackers to compromise the web server or data first, then work backwards to gain access to administration features and other user accounts.

The 'Recommendation' sections of this report provides high level advice on highest priority remedial actions to reduce risks associated with 'Concrete2.0'. An overview of the strength and weaknesses is also provided to give insight into where the software development processes are work well and where there are opportunities for improvement.

Full details of each issue identified during testing, along with guidance and solutions for their remediation, are provided in the main technical section of this report, with a concise overview of the more important issues appearing in the Technical Summary.

## **1.3 Recommendations**

### **RECOMMENDED ACTION PLAN**

#### **Use a more robust approach for input validation**

Prevent SQL Injection, Cross-site scripting and file upload attacks by ensuring that all input is validated when received by the application and correctly escaped when the application send it to external systems (namely when the application communicates with the database, user's browser or the underlying file system). The web application should be modified so that it applies a layer of filtering to all user-supplied data, before it is saved by the system. In particular, ensure that file upload functionality is implemented according to industry good security practice guidelines - as described in this report.

#### **Implement Cross-site Request Forgery Protection**

A unique and random token should be included within sensitive functions to prevent an attacker forging links that could be used to carry out operations on a user's behalf, without their knowledge.

#### **Implement a robust approach to password management**

Strict rules governing the setting of passwords should be created and a policy implemented that enforces the use of strong and complex values, as per the recommendations contained within this report. It is important that passwords are not re-used across accounts on the same systems, or across multiple servers, to lessen the likelihood of a higher number of individual systems or components being compromised.



**Ensure that sensitive data is encrypted**

Remove any communication channels that are not encrypted and replace them with secure versions. This report provides detailed recommendations for configuring encrypted access (HTTPS) in line with good security practice.

## 2. Project Summary

Members of the Cisco Advisory team have served as trusted business advisors, cyber security leaders, and technical experts in a wide range of roles. Together we use our vast experience in cyber security, risk management, and technical innovation to help our clients across every industry advance their business objectives.

### 2.1 Project Scope

The following URL was in scope:

- [REDACTED]

The Team assessed the 'Concrete2.0' web application from both authenticated and unauthenticated perspective. The following administrative accounts were used to assess the 'Admin' role:

- [REDACTED]
- [REDACTED]

The following two accounts were used to assess the 'User' role:

- [REDACTED]
- [REDACTED]

### 2.2 Project Teams

Cisco Project Team		
Team Member	Project Role	Contact Information
Simon Quatrini	Team Lead	
sdytrych	Team Member	sdytrych@portcullis-security.com

Test Company Project Team		
Team Member	Project Role	Contact Information
Test Contact	Client Title	email@addr.ess

## 3. Technical Analysis

### 3.1 Technical Summary

The Team assessed the web applications from both unauthenticated and authenticated perspectives, finding 4 issues rated as 'High' in terms of their potential severity (the remaining 13 issues were rated 'Medium', 'Low' or 'Informational'). A concise overview of the most notable findings is provided below by way of introduction to the main technical section of this report.

The Team considered that the following specific discoveries should be highlighted:

- The web application failed to appropriately sanitise user input making the site vulnerable to Cross-site scripting attacks. An attacker managing to obtain valid credentials could inject code or text into a web page in a non-permanent way. This could make targeted users believe the website has been defaced or allow users to be more effectively targeted by phishing attacks that steal usernames and passwords.
- The web application suffered from a vulnerability that would allow an attacker to issue commands on the back-end database server. This could result theft of or modification of data and could allow compromise of the database server, under certain conditions.
- It would be possible for an unauthenticated attacker to enumerate valid usernames, which they could then target via password guessing/brute-force attacks.
- It was possible to upload dangerous file types to the applications.
- The password policy was weak, allowing easily guessable passwords such as 'a' or '123456' to be set. It was possible to use weak passwords in the registration or in the 'Change password' functionality (issue [4.10](#)).

The Team identified weaknesses in the input validation routines, making it possible to inject malicious JavaScript code into a user's browser under certain specific circumstances (issue [4.13](#)). A SQL Injection was identified in the 'News' section of the web application under assessment (issue [4.1](#)) which allowed the Team to access all the database information and to escalate privileges by cracking the 'sa' account's password. The avatar upload functionality was not sufficiently protected against malicious file-type (issue [4.3](#)): the Team was able to upload a PHP script instead of an image and execute it in the hosting server. Finally, a remote command execution in the 'show\_file.php' page allowed the Team to read, edit or delete any file in the web root folder (issue [4.2](#)).

In order to protect against these attacks the application needs to prevent potentially malicious payloads being processed.

Communications with the web site were generally well secured, but the following important observations were made:

- The web server was accessible over HTTP as well as HTTPS (see issue [4.5](#))
- The web server did not instruct the user's browser to communicate over a secure connection only (see [4.4](#))
- The web applications did not enforce the 'Secure' flag on cookies, meaning that they could be transmitted unencrypted over the network (see [4.9](#))

These relatively small number of shortcoming in the security of network traffic could leave users of the site vulnerable to 'SSLstrip' style attacks, where an Man-in-the-Middle modifies traffic in such a way that the legitimate user never uses SSL at all. It would be possible to take over a user's account in this scenario.

An SSL good practice guide has been included in Appendix [Appendix B: General SSL Recommendations](#) at the end of this report. The recommendations therein can be adopted along with those appearing in the individual issues themselves.

Other security misconfigurations were identified during the assessment: for example, the Team was able to enumerate users by observing the responses from the registration page when valid and invalid input was submitted (issue [4.8](#)).

It is recommended that the application take advantage of certain browser security enhancements as detailed in issues 4.4 and 4.15.

Finally, a number of less serious issues were identified, for example incidences of information disclosure. Whilst the majority of these may not in themselves represent a direct threat to security, they should be addressed in order to prevent an attacker acquiring information that could enable them to plan more sophisticated attacks.

## 3.2 Summary of Findings

### STRENGTHS

Session management and page access controls were sufficiently robust to prevent direct privilege escalation attacks between user account and from user account to administrator accounts.

'Concrete2.0' correctly presented Directory Traversal attacks by sanitising user-supplied data.

The SSL services was configured accordingly to good security practice - though see issues in this report about forcing all data over SSL.

A dedicated pre-production environment was made available for security testing, allowing issues to be identified and fixed before being exposed to the Internet.

### WEAKNESSES

#### Improper Neutralisation of Input

##### DESCRIPTION

The web application does not sanitise (or incorrectly sanitises) user-supplied input before it is rendered on web pages accessed by other users or sent into an SQL statement. In addition it would be possible for an attacker or malicious user to upload or transfer dangerous file types that could be automatically processed within the environment.

##### SOLUTION

All data arriving at the server should be treated as untrustworthy, therefore, the web application should be modified to apply a layer of filtering to all user-supplied data before it is saved by the system or it is used inside an SQL statement. This data should also be properly encoded during its presentation as content. Where possible, structured mechanisms that automatically enforce the separation between data and code should be used, as these may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. It should be assumed that all user-supplied input is malicious and, therefore, strong input validation mechanisms should be in place. A whitelist of acceptable inputs that strictly conform to specifications and that rejects any input that does not strictly conform (or transforms it into an acceptable type) should be considered.

#### Cross-site Request Forgery

##### DESCRIPTION

With no protection against Cross-site Request Forgery attacks in place, an attacker could potentially impersonate an authorised user to carry out a range of malicious actions.

##### SOLUTION

The web application should be modified to check that a request has come from a user-generated process such as completing a form or clicking a link. In effect, each transaction to be processed should carry a unique identifier.

### Site Uses HTTP and HTTPS

#### DESCRIPTION

The presence of the HTTP site along with some misconfiguration in how the browser is instructed to treat cookies and use the HTTPS site leaves users more exposed to attack than necessary - despite the otherwise good configuration of the SSL stack of the HTTPS site.

#### SOLUTION

Follow the advice in this report about instructing browsers to treat cookies more securely and to always use the HTTPS site.

### Weak Password Requirements

#### DESCRIPTION

The password policy in place is insufficient to ensure that appropriately secure passwords are set.

#### SOLUTION

Ensure that all accounts have a strong password set. Passwords should have an appropriate complexity based on the type and level of access and the systems on which they can be used. Each password should be created from a large character set that forces the user to select a combination of upper, lower and special case characters as well as numbers. In addition, they should not be based on a dictionary word, the username or the associated system.

### Insufficient Session Expiration

#### DESCRIPTION

If sessions are not set to expire, an attacker able to steal a session would theoretically have unlimited time in which to attack a user's session.

#### SOLUTION

Ensure all session tokens are invalidated at the server side when users log out.

## INDEX OF FINDINGS

Finding Title	Severity Rating	CVSS Score
1. Web Application Vulnerable To SQL Injection	<b>CRITICAL</b>	<b>9.8</b>
2. Web Application Allows Arbitrary Command Execution	<b>HIGH</b>	<b>8.8</b>
3. Web Application Allows Arbitrary File Uploads	<b>HIGH</b>	<b>8.8</b>
4. HTTP Strict Transport Security (HSTS) Not Enabled	<b>MEDIUM</b>	<b>6.5</b>
5. Web Application Available Over Unencrypted Channel	<b>MEDIUM</b>	<b>6.5</b>
6. Sessions Not Expired Server Side On Logout	<b>MEDIUM</b>	<b>5.4</b>
7. Web Application Allows Concurrent Logins	<b>MEDIUM</b>	<b>5.4</b>
8. Web Application Allows User Enumeration	<b>MEDIUM</b>	<b>5.3</b>
9. Web Application Does Not Use 'secure' Cookies	<b>MEDIUM</b>	<b>5.3</b>
10. Web Application Implements Weak Password Policy	<b>MEDIUM</b>	<b>5.3</b>
11. Web Application Vulnerable To Cross-site Request Forgery Attacks	<b>MEDIUM</b>	<b>5.3</b>
12. Web Application Vulnerable To Reflective Cross-site Scripting	<b>MEDIUM</b>	<b>5.1</b>
13. Web Application Vulnerable To Stored Cross-site Scripting	<b>MEDIUM</b>	<b>4.9</b>
14. Web Application Does Not Display Last Successful And Unsuccessful Login	<b>NONE</b>	<b>0.0</b>
15. Web Application Does Not Specify Content Security Policy (CSP)	<b>NONE</b>	<b>0.0</b>

## 4. Web Application Assessment

### 4.1. Web Application Vulnerable To SQL Injection

<b>Severity Rating</b>	<b>CRITICAL</b>	<b>CVSS Score</b>	<b>9.8</b>
<b>CWE Category</b>	CWE-89: Improper Neutralisation of Special Elements used in an SQL Command (SQL Injection)		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:H/I:H/A:H/S:U/UI:N		
<b>Affected Components</b>	██		

#### Specific Detail

The Team identified a vulnerability to SQL Injection attacks resulting from a lack of sanitisation of the client data processed in SQL queries sent to the back-end database.

#### Impact

An attacker gaining sufficient network access could manipulate the data sent to the server and affect the SQL queries being processed, potentially enabling them to:

- Extract sensitive information, including (but not limited to) authentication credentials and personal details. Such information could be sold by the attacker to other malicious individuals, used in other attacks (as the same password is often used across systems) or released publicly to damage the organisation's reputation.
- Modify data within the current database.
- Access other databases.
- Execute remote code, as the application was using the 'SA' account to connect to the database. This would give the attacker full and complete control of the server on which the database was running.
- Modify content within the application. If this was possible, the attacker could add malicious code to the application, which could then be used to deliver malware or exploit issues within client browsers.

#### Recommendation

Cisco strongly recommends that the application source code is reviewed to ensure that parametrised queries are used in all instances where it talks to the database, and that all user-supplied input is sanitised, prior to the passing of data in SQL queries.

Note: It is important to ensure that the connection is switched to the least privileged database user instead of 'root'.

#### Steps to Replicate

Follow these guided steps to replicate the issue:

- 1) Access the 'News' section
- 2) Click on the following malformed URL that extract the MySQL version via SQL Injection:

```
https://testuat.clientapp.com/news.php?id=-  
1/**/UNION/**/ALL/**/SELECT/**/version(),2,3,4/*
```



## 4.2. Web Application Allows Arbitrary Command Execution

<b>Severity Rating</b>	<b>HIGH</b>	<b>CVSS Score</b>	<b>8.8</b>
<b>CWE Category</b>	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')		
<b>CVSS Base</b>	AV:N/AC:L/PR:L/C:H/I:H/A:H/S:U/UI:N		
<b>Affected Components</b>	[REDACTED]		

### Specific Detail

The Team identified that the web application allowed arbitrary commands to be executed on the host.

Component	Details
[REDACTED]	This vulnerability was identified in: <ul style="list-style-type: none"> <li>[REDACTED]</li> </ul>

### Impact

By exploiting this vulnerability, an attacker can execute any number of commands on the host, including system commands. The attacker could potentially access system files and perform privilege escalation techniques to gain a higher level of access to the application and its data, or to completely compromise the machine that the application is hosted on.

### Recommendation

Cisco recommends that all facilities to execute commands through the web application are removed. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a white-list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules.

Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). A blacklist is likely to miss at least one undesirable input, especially if the code's environment changes. This can give attackers enough room to bypass the intended validation. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

### Steps to Replicate

Follow these guided steps to replicate the issue:

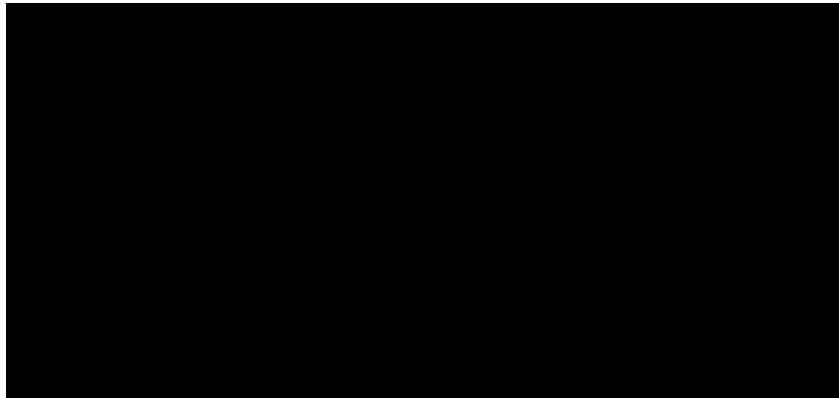
- 1) Open the "Terms and Conditions" page from the homepage
- 2) Click on any available document to consult
- 3) The following request will be made:

[Redacted]

- 4) Now perform the following malformed request to show the content of "/etc/passwd" file in linux (note %23 is encoding of #, the shell comment character)

[Redacted]

- 5) The system will execute the injected command, returning the content of the file.



*Figure 1 - The image is showing the server's response with the /etc/passwd content*

4.3. Web Application Allows Arbitrary File Uploads			
Severity Rating	<b>HIGH</b>	CVSS Score	<b>8.8</b>
CWE Category	CWE-434: Unrestricted Upload of Dangerous File Types		
CVSS Base	AV:N/AC:L/PR:L/C:H/I:H/A:H/S:U/UI:N		
Affected Components	[REDACTED]		

**Specific Detail**

The Team discovered that users were able to upload files of any type.

**Impact**

Permitting the uploading of arbitrary files could result in highly damaging content such as malware, indecent images, viruses and/or pirated software being uploaded and stored, and later downloaded. In addition, the storage of such material could quite possibly have serious legal implications for the hosting organisation.

In this case, an attacker could exploit the functionality to upload server scripts which, when requested by a browser, would execute code on the server.

**Recommendation**

Cisco recommends that all content uploaded to the web server by users is checked for validity, i.e. that there is a correctly formatted image file and a valid file extension. Most of the time, just checking for the file extension is not enough.

Cisco also recommends that the directory in which the uploads are saved is prevented from being able to execute any files it contains, so that any malicious executable files uploaded by an attacker could never be run i.e. having the web application to choose a safe file-name extension or disable the execution permission on the new uploaded files. In addition, when possible, the location of the uploaded file should be outside of the web root and accessed by other means.

**Steps to Replicate**

Follow these guided steps to replicate the issue:

- 1) Login with valid credentials via /login.php
- 2) Click on "Account -> Change avatar"
- 3) In the Upload form select an image and, before submitting the form, intercept the request with a proxy (the tool 'Burp' was used during testing)
- 4) Edit the body of the request with the following values (note the filename and contents have been changed):

```
-----735323031399963166993862150
Content-Disposition: form-data; name=[REDACTED]
[REDACTED]
-----735323031399963166993862150
```

---

```
Content-Disposition: form-data; name=[REDACTED]; filename=[REDACTED]
Content-Type: application/php
```

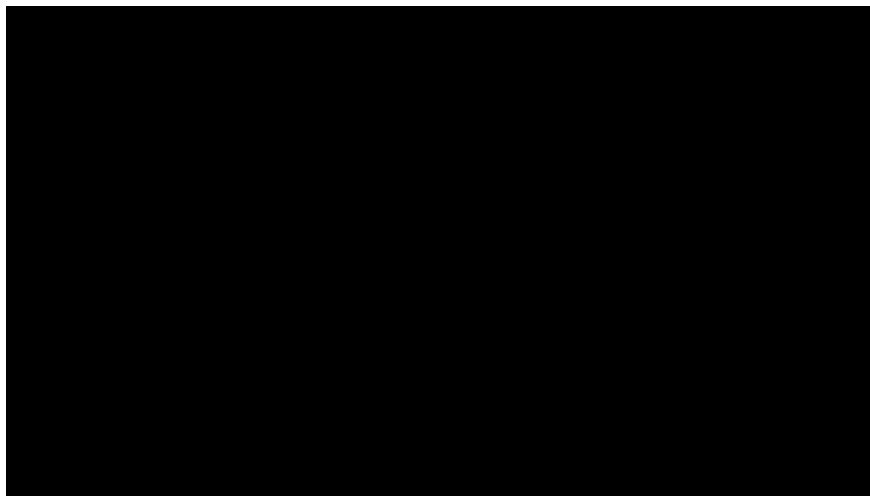
```
GIF87a <?php passthru($_GET['cmd']); ?>
```

```
-----735323031399963166993862150
```

5) The file will be directly uploaded to the '/public/' folder with the extension specified by the user in the "filename" (avatar\_119191283.php).

Since the '/public/' folder also allows execution permission, it's possible to execute command as follow (note that %26%26 is the encoding for &&):

[REDACTED]



*Figure 2 - The image is showing the remote command execution through the upload functionality*

#### 4.4. HTTP Strict Transport Security (HSTS) Not Enabled

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>6.5</b>
<b>CWE Category</b>	CWE-311: Sensitive Data Not Encrypted		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:L/I:L/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

#### Specific Detail

The Team observed that the web server did not instruct the user's browser to communicate over an HTTPS connection only; an HTTP header similar to the following was not returned in response to HTTPS requests:

```
Strict-Transport-Security: max-age=NNNNNN
```

Note: Browsers must be HSTS-compliant (for example, Internet Explorer, Chrome, Firefox, etc) to take advantage of this security feature.

#### Impact

Whilst there is no direct security impact associated with failing to support this feature, HSTS has a role to play in achieving strength-in-depth. It will prevent compliant browsers from being tricked into sending sensitive data over an insecure connection, and will also reduce the scope for users to make poor decisions about any related SSL issues. Hence, this feature mitigates certain other vulnerabilities such as the failure to implement 'secure' cookies, and also strengthens the system's resistance to certain downgrade attacks.

#### Recommendation

Cisco recommends that the server is reconfigured to support HSTS. Furthermore, a redirect response should be immediately sent for requests going over HTTP to enforce all traffic to go through the HTTPS connection.

This can be achieved via Apache's 'mod\_headers' by including the following line in the Virtualhost:

```
Header add Strict-Transport-Security: "max-age=██████████"; includeSubDomains
```

Additionally, the following code should be added within the Virtualhost that handles HTTP connections.

```
ServerAlias *
RewriteEngine On
RewriteRule ^(.*)$ ██████████ ██████████
```

#### 4.5. Web Application Available Over Unencrypted Channel

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>6.5</b>
<b>CWE Category</b>	CWE-311: Sensitive Data Not Encrypted		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:L/I:L/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

#### Specific Detail

The Team identified that the web application was available over HTTP but redirected to HTTPS.

#### Impact

A malicious user on the same network as the user or who controls a segment of the network between the user and the server could intercept a request and launch a "Man-In-The-Middle" (MITM) attack against the user's visit to the site.

Once the attacker has performed a MITM attack they will have two connections; one in plain text between the victim and the attacker, and one encrypted between the attacker and the server. If the user fails to notice that the padlock icon is missing in their browser, all transferred data could be monitored/modified by the attacker. This will lead to the loss of their credentials and other sensitive content. Several tools to perform this kind of attack are freely available on the Internet.

#### Recommendation

Cisco recommends that the application host is modified so that it is only available over an encrypted HTTPS channel.

As this site contains sensitive data, it is recommended that the HTTP version of the site is disabled completely. Ideally this application should be on a domain which is only ever linked to from other sites which enforce HTTPS in the URL. For example, bankX.com would exist on both port 80 and 443 using HSTS and would redirect to deliver secure but non-sensitive content to the user. This would then link to <https://onlinebanking.bankX.com>, which is only available on port 443, with this enforced by enabling the HTTP Strict Transport Security (HSTS) headers in the web server.

#### 4.6. Sessions Not Expired Server Side On Logout

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>5.4</b>
<b>CWE Category</b>	CWE-613: Insufficient Session Expiration		
<b>CVSS Base</b>	AV:N/AC:L/PR:L/C:L/I:L/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

#### Specific Detail

The Team observed that sessions were not expired on the server side when users logged out.

#### Impact

An attacker managing to compromise a user's authentication cookie could continue to use it after the user had logged out. The attacker would then be able to lock the user out of their own account by changing the authentication details, and also perform other arbitrary actions using the legitimate user's privileges.

#### Recommendation

Cisco recommends that the session cookies are not only removed from the client's browser upon the user logging out, but that they are also invalidated on the server to prevent them being reused.

#### Steps to Replicate

Follow these guided steps to replicate the issue using an intercepting HTTP proxy that can replay requests (Burp was used during testing):

- 1) Make an authenticated request to the application, note the response and make a copy of the complete request (including cookies).
- 2) Logout of the application.
- 3) Replay the saved request and observe the response is the same as when the user is logged in.

#### 4.7. Web Application Allows Concurrent Logins

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>5.4</b>
<b>CWE Category</b>	CWE-724: Insecure Session Management		
<b>CVSS Base</b>	AV:N/AC:L/PR:L/C:L/I:L/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

#### Specific Detail

The Team discovered that the web application allowed multiple concurrent logins to the same account.

#### Impact

Allowing concurrent logins gives an attacker the opportunity to access a user account (if the authentication details have been exposed) without the user's or system administrator's knowledge. This makes the detection of an account compromise much more difficult. Concurrent logins also hamper any investigation into a security breach, as it is not possible to be sure who has actually performed an action if the authentication details have been compromised.

#### Recommendation

Cisco recommends that the application is modified to prevent concurrent logins. Prior to this, if a second concurrent login is detected then the appropriate people within the organisation should be informed as well as the users logged into the account.

Note: At each login, users should be informed of the time at which they last logged in, to allow them to identify whether their account has been used in the meantime (it is also imperative that this message includes information about who to contact if they believe their account has been compromised).



#### 4.8. Web Application Allows User Enumeration

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>5.3</b>
<b>CWE Category</b>	CWE-204: Response Discrepancy Information Exposure		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:L/I:N/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

#### Specific Detail

The Team observed that different responses were generated by the 'Register new account' page based on whether or not the user-supplied input in the email field corresponded to a valid user account.

#### Impact

This could allow an attacker to enumerate valid email addresses in preparation for brute-force and/or phishing attacks.

#### Recommendation

Cisco recommends that the same response is generated for both valid and invalid email address within the registration form. In some cases like this one, it wouldn't be possible to let user proceed if the same e-mail address is already registered. A proposed solution is to implement a CAPTCHA system on the registration form to prevent automated brute-force attacks.

#### Steps to Replicate

Follow these guided steps to replicate the issue:

- 1) Use the 'Register a new account' functionality
- 2) Input an already existing email address and observe the error message
- 3) Input a new email address and observe the response

#### 4.9. Web Application Does Not Use 'secure' Cookies

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>5.3</b>
<b>CWE Category</b>	CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:L/I:N/A:N/S:U/UI:N		
<b>Affected Components</b>	[REDACTED]		

#### Specific Detail

The Team observed that cookies were issued without the 'secure' flag set. The details below show the 'Set-Cookie' line from the HTTP response, which instructs the user's browser to create a new cookie to be returned in subsequent HTTP requests.

Component	Details
[REDACTED]	Set-Cookie: [REDACTED]

#### Impact

An attacker may be able to exploit this vulnerability to capture the cookies from a client's browser, as cookies not marked as 'secure' will be transmitted via HTTP connections in an unencrypted format. An attacker with sufficient network access could eavesdrop network traffic to capture these, then use them to hijack the user's session.

#### Recommendation

Cisco recommends that the web application is reconfigured to use 'secure' cookies.

For pages accessed over HTTPS, the following PHP code can be used to set the 'secure' attribute on the 'PHPSESSID' cookie:

```
session_set_cookie_params(null, null, null, true);
session_start();
```

Ideally, the 'php.ini' file would be used to specify that all cookies are 'secure' (by setting 'session.cookie\_secure' to 'True').

## 4.10. Web Application Implements Weak Password Policy

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>5.3</b>
<b>CWE Category</b>	CWE-521: Weak Password Requirements		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:L/I:N/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

### Specific Detail

The Team discovered that the web application implemented a weak password policy, allowing users to set passwords such as:

- ██████████
- ██████████
- ██████████

### Impact

Allowing weak and predictable passwords to be used dramatically increases the chance of an attacker being able to guess the password of an active account. The actual impact of any account compromise would depend on the type of account the attacker managed to compromise.

### Recommendation

Cisco recommends that an appropriate password policy consisting of a defined set of rules is implemented. Current good practice dictates that passwords should:

- Be a minimum of 9 characters in length.
- Consist of a mix of upper and lower case characters, at least one number and at least one non-alphanumeric character.
- Not contain the username or application name.
- Not be based on a dictionary word.

Note: Simply adding several numbers as a prefix and/or suffix to a word does not constitute effective protection (either online or offline).

### Steps to Replicate

Follow these guided steps to replicate the issue:

- 1) Login with valid credential on the website
- 2) Click on "Account -> Change password"
- 3) Input a new and weak password like ██████████
- 4) Submit the request and observe the weak password is allowed



## 4.11. Web Application Vulnerable To Cross-site Request Forgery Attacks

<b>Severity Rating</b>	<b>MEDIUM</b>	<b>CVSS Score</b>	<b>5.3</b>
<b>CWE Category</b>	CWE-352: Cross-site Request Forgery		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:N/I:L/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

### Specific Detail

The Team discovered that no protection against Cross-site Request Forgery attacks was implemented, resulting in the Team being able to:

- Change user's password
- Change user's details
- Cause another user to log in using a chosen account

### Impact

Cross-site Request Forgery exploits the way in which HTTP and web browsers work.

Due to the fact that HTTP is a stateless protocol, and that web browsers will include all relevant cookies for the domain that a request is for, if a user was logged into the application and the attacker sent a link that the user duly followed (or the attacker tricked them into following a link on a page), the user's browser would include all the cookies (including the session cookies) in the request. The attacker's link would then be executed with the user's privileges.

Lack of CSRF protection on the login page is significant in the context of the application tested. The site was also found to be vulnerable to authenticated Cross-site scripting attacks (see issues [4.12](#) and [4.13](#)). It is therefore beneficial to an attacker to first cause a victim to be logged in before triggering the Cross-site scripting vulnerability. This approach is sometimes called a "Session Donation" attack.

### Recommendation

Cisco recommends that the web application is modified to check that a request has come from a user-generated process, such as completing a form or clicking a link. In effect, each transaction to be processed should carry a unique ID value.

In addition, it is recommended that all functions only transmit their data via POST requests and that when each form is accessed a random value is set. This random value should then be added to the form (normally via a hidden field) and as a value within the user's session on the server side. When the application processes the required POST, it should check that the value hidden in the form and the value stored within the user's session are the same; if they are not, the request should be rejected.

### Steps to Replicate

Follow these guided steps to replicate the issue:

- 1) Create an HTML file called 'csrf.html' with the content specified below.

- 2) Login to the application.
- 3) Use the browser menu to open the 'csrf.html' file in a new tab.

```
<html>
<body>
<form action=[REDACTED] method="POST">
<input type="hidden" name=[REDACTED] value=[REDACTED] />
<input type="hidden" name=[REDACTED] value=[REDACTED] />
<input type="submit" value="Submit request" />
</form>
<script>
document.forms[0].submit();
</script>
</body>
</html>
```

- 4) The password for the logged-in user will be changed in [REDACTED]

4.12. Web Application Vulnerable To Reflective Cross-site Scripting			
Severity Rating	<b>MEDIUM</b>	CVSS Score	<b>5.1</b>
CWE Category	CWE-79: Improper Neutralisation of Input During Web Page Generation (Cross-site Scripting)		
CVSS Base	AV:N/AC:L/PR:N/C:N/I:L/A:N/S:U/UI:N		
CVSS Temporal	E:H/RL:O/RC:C		
Affected Components	[REDACTED]		

**Specific Detail**

The Team identified that user-supplied input was not sufficiently sanitised. The following forms allowed malicious content to be injected into the site:

Component	Details
[REDACTED]	Affected page: [REDACTED] Affected parameter: 'id'

**Impact**

An attacker could exploit this flaw to get active HTML or script code executed in an authenticated user's browser. Cross-site Scripting may be used to perform attacks such as session hijacking by invoking the user's browser to send information stored in their cookies (such as a session identification token) to an arbitrary location controlled by the attacker. Furnished with this information the attacker could immediately access the site, masquerading as the authenticated user who viewed the page containing the malicious code. The attacker would then be able to perform actions as the authorised user, subject to their role, which could include viewing sensitive data, modifying profile information and making transactions.

This vulnerability could also be leveraged in a "phishing" attack, whereby the attacker adds additional HTML code to create a false login page within the vulnerable page, which posts the data to a server controlled by the attacker. The attacker could then redirect the user back to the original server, thus giving the illusion that the login was secure and genuine. This could also be achieved by redirecting the user to a false login page on the attacker's server rather than adding the code to a page that already exists. This is critical, because if the attacker could host a "phishing" website in a domain with a valid SSL certificate, there would be no way for a user to spot the attack.

A variation of the "phishing" attack described above would be to inject code to completely rewrite the genuine page, defacing the site and possibly having a detrimental impact on the reputation of the company.

Finally, an attacker could use Cross-site Scripting to exploit vulnerabilities within web browsers. The outcome of such an attack would depend on the exploits used, but in a worst case scenario the attacker could gain full control of a user's computer. Once that had been achieved it would be trivial for the attacker to install a keystroke logger and gain access to applications via the usernames and passwords they had acquired.

In the case of the current web application, the Cross-site Scripting was "reflective", meaning that a user

would need to follow a specially crafted link for the attack to be successful.

### Recommendation

Cisco recommends that all data sent by a client to the server is treated as untrustworthy, and that the application performs validation on all of the input. After validation, the application should encode all required characters before inserting them into the page. To be able to encode the data correctly according to the output location, Cisco recommends the use of a specialised library such as OWASP Enterprise Security API. Cisco also recommends referring to the OWASP XSS (Cross-site Scripting) Prevention methods.

### Steps to Replicate

Follow these guided steps to replicate the issue:

- 1) Log into the application as a normal user.
- 2) Browse the the following URL:

```
https://testuat.clientapp.com/employee/news.php?id=<script>alert('Reflective_XSS')</script>
```

- 3) Observe that an alert message appears.



4.13. Web Application Vulnerable To Stored Cross-site Scripting			
Severity Rating	MEDIUM	CVSS Score	4.9
CWE Category	CWE-79: Improper Neutralisation of Input During Web Page Generation (Cross-site Scripting)		
CVSS Base	AV:N/AC:L/PR:N/C:N/I:L/A:N/S:U/UI:N		
CVSS Temporal	E:F/RL:O/RC:C		
Affected Components	[REDACTED]		

### Specific Detail

The Team discovered that data supplied to the web application was permanently stored and could be retrieved later by other users. This is a normal feature of many applications, however, in this instance the application failed to restrict the type of data that could be stored and also failed to sanitise it, meaning that it could not be safely rendered by the browser.

The following forms allowed malicious content to be injected into the site:

Component	Details
[REDACTED]	Affected page: [REDACTED] Affected parameter: 'text'

### Impact

An attacker could exploit this flaw to get active HTML or script code executed in an authenticated user's browser. Cross-site Scripting may be used to perform attacks such as session hijacking by invoking the user's browser to send information stored in their cookies (such as a session identification token) to an arbitrary location controlled by the attacker. Furnished with this information the attacker will be able to access the site, masquerading as the authenticated user who viewed the page containing the malicious code. The attacker would then be able to perform actions as the authorised user, subject to their role, which could include viewing sensitive data, modifying profile information and making transactions.

This vulnerability could also be leveraged in a phishing attack, whereby the attacker adds additional HTML code to create a false login page within the vulnerable page, which posts the data to a server controlled by the attacker. The attacker could then redirect the user back to the original server, thus giving the illusion that the login was secure and genuine. This could also be achieved by redirecting the user to a false login page on the attacker's server rather than adding the code to a page that already exists. This is critical, because if the attacker could host a phishing website in a domain with a valid SSL certificate, there would be no way for a user to spot the attack.

A variation of the phishing attack described above would be to inject code to completely rewrite the genuine page, defacing the site and possibly having a detrimental impact on the reputation of the company.

Finally, an attacker could use Cross-site Scripting to exploit vulnerabilities within web browsers. The outcome of such an attack would depend on the exploits used, but in a worst case scenario the attacker could gain full control of a user's computer. Once achieved, it would then be trivial for the attacker to install a keystroke logger and gain access to applications via the usernames and passwords they had acquired.



#### 4.14. Web Application Does Not Display Last Successful And Unsuccessful Login

<b>Severity Rating</b>	<b>NONE</b>	<b>CVSS Score</b>	<b>0.0</b>
<b>CWE Category</b>	CWE-223: Omission of Security-relevant Information		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:N/I:N/A:N/S:U/UI:N		
<b>Affected Components</b>	████████████████████		

#### Specific Detail

The Team observed that details of the last successful and unsuccessful logins were not displayed upon successful authentication.

#### Impact

Without this information a user is unable to identify whether their account has been used without their permission, or whether an attacker has attempted to brute-force their credentials.

#### Recommendation

Cisco recommends that the web application is modified so that the last successful and unsuccessful login details are displayed at each login.

#### 4.15. Web Application Does Not Specify Content Security Policy (CSP)

<b>Severity Rating</b>	<b>NONE</b>	<b>CVSS Score</b>	<b>0.0</b>
<b>CWE Category</b>	CWE-673: External Influence of Sphere Definition		
<b>CVSS Base</b>	AV:N/AC:L/PR:N/C:N/I:N/A:N/S:U/UI:N		
<b>Affected Components</b>	[REDACTED]		

#### Specific Detail

The Team observed that the web server did not instruct the user's browser to restrict the sources from which assets (for example, scripts, styles, images or frames) were allowed to be loaded. An HTTP header similar to the following was not returned in response to requests:

[REDACTED]

#### Impact

Without this header, there would be an increased risk of successful Cross-site Scripting attacks should an attacker be able to inject HTML or JavaScript code into a server response.

#### Recommendation

Cisco recommends that the Content Security Policy (CSP) feature be used to improve resistance to Cross-site Scripting attacks by banning the use of inline scripts and styles, and limiting allowed asset sources to trusted locations. When implemented correctly, CSP can mitigate all but the most sophisticated Cross-site Scripting attacks.

Note: For effective protection, no inline scripts or styles should be used in pages, and should instead be moved to their own files.

# Appendices

---

## Appendix B: General SSL Recommendations

This appendix offers recommendations to aid in the secure configuration of SSL services. It also offers some sample implementations for commonly deployed SSL services. For full details of all the issues considered when these recommendations were made, please look at our SSL Good Practice Guide, which can be found at:

- <http://labs.portcullis.co.uk/whitepapers/ssl-good-practice-guide/>

### APPENDIX B.1: SAMPLE IMPLEMENTATIONS

#### APACHE

These settings were devised after consulting the documentation for Apache's mod\_ssl extension ([http://httpd.apache.org/docs/current/mod/mod\\_ssl.html](http://httpd.apache.org/docs/current/mod/mod_ssl.html)).

```
SSLProtocol -ALL +TLSv1.2 +TLSv1.1 +TLSv1
SSLHonorCipherOrder On
SSLCipherSuite ALL:!SSLv2:-SSLv3:!ADH:!DH:!kRSA:!MD5:!NULL:!PSK:RC4
SSLCompression off
Strict-Transport-Security: max-age=15768000 ; includeSubDomains
```

#### IIS

These settings were devised after consulting the documentation in Microsoft's Knowledge Base article 245030 (<http://support.microsoft.com/kb/245030>).

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1
.0\Server] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2
.0\Server] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128
/128] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/
128] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/
128] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/
128] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/
128] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/
128] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL] "
Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple
```

```
DES 168/168] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C
iphers\RC2_56/
56] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\C
iphers\DES_56/
56] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\K
eyExchangeAlgo
rithms\Diffie-Hellman] "Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\K
eyExchangeAlgo
rithms\PKCS] "Enabled"=dword:00000000
```

## APPENDIX B.2: RECOMMENDATIONS

Whilst it is acknowledged that there are security concerns associated with the use of SSL, adhering to the guidelines that follow when configuring SSL services will ensure that any risks are minimised. Although some of the issues considered are specific to certain uses of SSL, the advice given below is applicable wherever SSL is in use.

### CIPHER SUITES

When selecting a cipher suite, ensure that the symmetric keys are at least 128 bits in length and that asymmetric keys are larger than 1024 bits. Use only RC4 under TLSv1 and, wherever possible, ensure that AES-GCM or AES-EAX ciphers are used. The key exchange method should be EDH (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Diffie-Hellman Ephemeral).

### CONFIGURATION

SSLv2 must be disabled and the server configured to prefer TLSv1.2/TLSv1.1 connections. Ideally TLSv1/SSLv3 would be disabled, however, as most clients do not support TLS1.1/TLS1.2, TLSv1/SSLv3 can be enabled for compatibility but only using non-block ciphers.

Compression must also be disabled and, if side channel information leakage is a concern, implementing some form of packet padding/size adjustment at the service level should be considered.

### CERTIFICATES

Ensure that the certificate is current and signed by a trusted Certificate Authority using a strong hashing algorithm (not MD5).

### CLIENTS

SSL clients, including mobile applications, should make use of established SSL libraries. Certificate validation is key, as are the ciphers supported. The same rules apply here as on the server, namely that TLSv1.2 with AES-GCM or AES-EAX is used wherever possible and that only RC4 is used under SSLv3 or TLSv1.

Certificate pinning may be possible, such as that implemented in Chrome and Internet Explorer, which ensures that the certificate for a service is provided by a Certificate Authority authorised by the application itself. This ensures that even if a compromised or rogue Certificate Authority issues a valid certificate for a service, clients will reject it.

## Appendix C: Generic Assessment Methodology

### **FOR EACH SERVICE PERFORMED IN SUPPORT OF THIS REPORT, INCLUDE A SINGLE PAGE METHODOLOGY IN THE APPENDIX:**

At a minimum, ensure this methodology includes any methodology mentioned in the statement of work agreed to by the customer for this engagement. Request this from the Project Manager.

Ideally, you'll additionally document what you actually did (ensuring it does not contradict the SOW)

If the contractual methodology is lacking or missing, see the "Cisco Responsibilities" statement of work content within the documents at:

[http://gitlab.cisco.com/css\\_advisory/NAME\\_OF\\_SERVICE/sales/statement\\_of\\_work/](http://gitlab.cisco.com/css_advisory/NAME_OF_SERVICE/sales/statement_of_work/)

for material you can use to construct the methodology.

### **IN GENERAL, IT SHOULD INCLUDE THE FOLLOWING**

- target research: (e.g., attack surface, critical assets and operations, security sensitive functions, business and security requirements)
- threat research: (e.g., threat modeling, online research)
- assessment plan: develop an assessment plan based on the previous stages that does not negatively impact the customer
- plan execution: to determine if a security concern exists or not (e.g., vuln scanning, exploitation, config review, doc review, interview, etc )
- documentation: documenting and reporting testing activities and their results

### **ONCE WRITTEN, ENSURE YOUR NEW METHODOLOGY IS INCLUDED IN GITLAB SO THAT IT CAN BE ROLLED BACK INTO XDB**

**ONCE PEER REVIEW IS COMPLETE, PLEASE UPDATE THE XDB TASK WITH CHANGES MADE DURING THE PEER REVIEW TO ENSURE THAT THE INFORMATION IN XDB IS UP TO DATE WITH THE DELIVERABLE THAT WAS PROVIDED TO THE CLIENT.**



## Appendix D: Definition of Terms

Each finding identified during the assessment is allocated a Severity Level and CVSS 3.0 score; the Severity Level being directly derived from the CVSS 3.0 score as per the standard, as well as being described under the Specific Details, Security Impact and Recommendations headings, with an additional Steps to Reproduce header, where applicable. The ratings are based on the individual objective finding and not the subjective risk the issue may pose.

### CVSS

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS consists of 3 groups: Base, Temporal and Environmental.

Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics. These metric groups are described as follows:

- Base: represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and across user environments.
- Temporal: represents the characteristics of a vulnerability that may change over time but not across user environments.
- Environmental: represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

Cisco uses the CVSS 3.0 scoring mechanism and directly maps those to severity ratings for each finding, as defined in the CVSS 3.0 standard shown below:

Severity Rating	CVSS Score
Critical	9.0 – 10.00
High	7.0 – 8.9
Medium	4.0 - 6.9
Low	0.1 – 3.9
None	0.0

### CWE

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.

- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

Cisco applies a relevant CWE against each finding in order to allow for finding grouping, which is then used to generate the remediation action plan in the recommendations section of the report.



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



# Cisco Customer Experience



## ABC Environment Pentest

Internal Network Pentest Example Report

Technical Report

1.0



## About This Document

Document Information	
Author	Mark Jones
Change Authority	Cisco Systems Advanced Services
Client Reference	ABC Environment Pentest
Project ID	123123
Task Reference	INTERNAL_NETWORK_PENTEST_SAMPLE

Document History		
Version	Status	Comments
0.8	Cisco Internal	1st Draft
0.9	Cisco Internal	2nd Draft
1.0	Customer Document	Release

Document Review	
Reviewer	Version
Alex Murphy	0.9
Tim Smith	1.0



This document contains and constitutes the proprietary and confidential information of Cisco ("Cisco"). It is provided to Exemplum ("Company") subject to and in accordance with the terms of any agreement between Cisco and the Company regarding treatment of confidential information and/or licensing of proprietary information. This document also contains information that is highly sensitive confidential information of the Company and should be treated by representatives of the Company accordingly. This document may not be distributed by the recipient without the express permission of Cisco and the Company.

The contents of this document do not constitute legal advice. Cisco's offer of services or deliverables that relate to compliance, litigation, or other legal interests is not intended as legal counsel and should not be taken as such.

# Table of Contents

Table of Contents .....	4
1. Executive Summary.....	5
1.1 Introduction.....	5
1.2 Conclusions .....	5
1.3 Recommendations.....	7
RECOMMENDED ACTION PLAN .....	7
2. Project Summary.....	8
2.1 Project Scope .....	8
2.2 Project Teams.....	8
3. Technical Analysis.....	9
3.1 Technical Summary .....	9
3.2 Summary of Findings .....	9
STRENGTHS .....	12
WEAKNESSES.....	12
INDEX OF FINDINGS .....	15
4. Internal Infrastructure Assessment.....	17
Appendices.....	69
Appendix A: Internal Infrastructure Assessment.....	69
APPENDIX A.1: DEFAULT PASSWORDS PRESENT ON SERVER .....	69
APPENDIX A.2: IPMI PROTOCOL VULNERABLE TO PASSWORD HASH RETRIEVAL.....	69
APPENDIX A.3: SSL/TLS SERVICE USES EXPIRED CERTIFICATES.....	69
APPENDIX A.4: SNMP SERVER WEAK COMMUNITY STRING CONFIGURED.....	70
Appendix B: Definition of Terms .....	71
CVSS.....	71
CWE .....	72
Appendix C: Why Cisco Assessment and Penetration Team? .....	73

# 1. Executive Summary

---

## 1.1 Introduction

Exemplum engaged Cisco to perform an Internal Network Penetration Test of the ABC environment. A Network Penetration Test is a type of "ethical hacking" or "intrusion testing" approach for detecting computer system vulnerabilities that malicious attackers could use to exploit an application and compromise sensitive data. Cisco performed the assessment remotely from offices in San Francisco.

The internal assessment yielded 29 findings, including five (5) Critical-Risk, seven (7) High-Risk, and seventeen (17) Medium-Risk findings.

Cisco performed the Internal Network Penetration Test remotely via VPN. The agreed scope of work was completed on schedule. Cisco wishes to thank Tina Bloggs (Head of Vulnerability Management, Exemplum) for her support, which enabled Cisco's consultants to complete the engagement as planned.

## 1.2 Conclusions

The ABC environments embody sizeable information security risk due to the quantity and old age of the software present. Of the twenty-nine (29) findings in the internal network assessment, approximately twelve (12) findings also reflect outdated or unmaintained software or configurations, some of which have significant vulnerabilities. Maintenance of technical environments is critical to stable and secure operation, and this should be a primary goal of Exemplum.

At a high level, the most important recommendation Cisco can make is to review patch and configuration management processes to ensure that each component receives maintenance and upgrades on a timely basis. Whilst the individual findings documented herein reflect opportunities for incremental improvement, devoting attention to supporting processes and activities will, over time, reduce technical risk and improve maintainability of the ABC environment.

### Critical Risk Findings

Two (2) Critical-Risk Findings pertain to outdated versions of VMware vCenter Server and Microsoft Remote Desktop. An attacker might be able to exploit vulnerabilities in systems and gain a significant level of access to the vulnerable systems. Bringing these products up-to-date should be a priority.

Two (2) Critical-Risk findings were related to the use of default passwords on user accounts. Attackers would be able to gain access to these systems without a significant level of effort; therefore, review and remediation of the configurations of these systems would help improve security posture.

The remaining Critical-Risk finding relates to publicly available git repositories that contain network device configurations. Proper management of sensitive files will protect them from accidental disclosure.



## High Risk Findings

All seven (7) High-Risk findings relate to outdated installations of Dropbear SSH Server, Dell iDRAC7, VMWare ESXi, Microsoft SQL, PHP, Microsoft Windows, and OpenSSL. These products provide useful and important functionality, but due to their old age and quantity of known security issues, they might expose that functionality and data to abuse and theft. Bringing these products up-to-date should be a priority.

## Medium Risk Finding

Six (6) vulnerabilities relate to outdated installations of Apache Tomcat, OpenSSH, Apache, libssh, NTP, and APC InfraStruxure PDU Web Management Interface. Although these are rated as lower risk than the packages listed above, they share a necessity to maintain them up-to-date.

Six (6) vulnerabilities involve aspects of configuration, including information disclosure over the IPMI protocol, SMB encryption capabilities, SNMP community strings and functionality, and NTP functionality. Proper management of keys and secrets will protect them from disclosure.

Three (3) findings identify protocols that can disclose data and credentials as well as provide access to other hosts via plain text protocols or unobstructed views via network cameras. There are encrypted protocols and utilities available as alternatives, as well as more robust authentication options, and migration to these will further protect data functionality from exposure.

One (1) firewall bypass permits unrestricted Layer 3 communication between the ABC internal network and external hosts via DNS requests. Whilst IP connectivity might be an extreme example of DNS abuse, data can be exfiltrated from the environment with simple DNS requests.

One (1) finding of expired TLS certificates weakens the environment by conditioning users to ignore certificate errors. A user who ignores a certificate error might unwittingly choose to interact with a hostile host that also presents a certificate validation error.

## Summary

Cisco recommends that Exemplum review these findings relative to functional and business requirements, and then develop and implement a prioritized action plan to remediate risks that fall outside Exemplum's risk appetite.

## 1.3 Recommendations

### RECOMMENDED ACTION PLAN

#### Implement a robust approach to password management

Strict rules governing the setting of passwords should be created and a policy implemented that enforces the use of strong and complex values, as per the recommendations contained within this report. It is important that passwords are not re-used across accounts on the same systems, or across multiple servers, to lessen the likelihood of a higher number of individual systems or components being compromised.

#### Configure systems in line with security best practices

Poor configuration control could enable an attacker to obtain a foothold within the network or environment. Poor configuration includes the retaining of vendor-supplied default settings and/or passwords, which can often be easily guessed, and services being enabled unnecessarily.

All systems within the ABC environment should be reviewed and their configurations brought into line with industry good security practice guidelines. In addition, strict change control should be applied with regards to all production systems.

#### Control resources throughout their lifetime

Whilst it is important to configure systems in-line with good industry practice at the point of commissioning, failure to maintain the system's security level over time will lead to a degradation which might undermine any previous hardening that has been performed.

It is therefore recommended that systems be subjected to regular reviews designed to identify:

- Missing patches
- Changes to the initial configuration as a result of software installation
- Insecure use cases which might result in passwords or other sensitive information being disclosed
- Further changes that can be made to the configuration in light of recognised improvements in good security practice

#### Implement and adhere to secure development practices

Any web application to be deployed into a production environment should be checked against secure development techniques and be the subject of a full source code review, prior to live system deployment.

## 2. Project Summary

Members of the Cisco Advisory team have served as trusted business advisors, cyber security leaders, and technical experts in a wide range of roles. Together we use our vast experience in cyber security, risk management, and technical innovation to help our clients across every industry advance their business objectives.

### 2.1 Project Scope

The following network range provided by Exemplum was considered in-scope for the Internal Network Penetration Test:

- [REDACTED]

### 2.2 Project Teams

#### Cisco Project Team

Team Member	Project Role	Contact Information
Mark Jones	Team Lead	mj12345@cisco.com

#### Exemplum Project Team

Team Member	Project Role	Contact Information
Tina Bloggs	Head of Vulnerability Management	tina@exemplum.com

## 3. Technical Analysis

---

### 3.1 Technical Summary

The assessment findings fall into several categories:

- Outdated software
- Incomplete configuration maintenance
- Plain text network protocols
- Weak encrypted protocols
- Management of secrets
- Use of default configurations
- Denial-of-service

Application of these categories is explored in the technical summary for the Internal Penetration Test.

### 3.2 Summary of Findings

#### Technical Summary

Cisco performed an Internal Network Penetration Test against Exemplum's ABC network. From an internal perspective, Cisco observed a weak security posture. Compared to the findings in the report from the previous year, there were very few findings that were remediated before this year's assessment. Cisco identified a total of twenty-nine (29) findings, including five (5) Critical-Risk, seven (7) High-Risk, and seventeen (17) Medium-Risk findings.

#### Critical-Risk Findings

**Default Password In Use: Dell iDRAC:** Cisco identified a Dell iDRAC server that used known default credentials for authentication. This could allow an attacker to instantaneously gain the account's permissions without the use of time-consuming attacks, such as brute-force attacks and opens the door for a series of potentially more damaging attacks.

**Default Passwords Present On Server:** Cisco identified multiple servers that used known default credentials for authentication. This could allow an attacker to immediately gain access to the account and potentially use the vulnerable system as a pivot point to launch further attacks.

**Web Application Has Public Git Repositories Available:** Cisco identified multiple public repositories that served as rolling backups for network device configurations. This included sensitive information such as secret hashes, usernames, hostnames, etc. and could allow an attacker to compromise those network devices with the information stored in the public Git repositories.

**Insecure Software Version: VMware vCenter Server:** Cisco identified a vulnerable version of VMWare vCenter Server that was vulnerable to Server-side Request Forgery (SSRF) and arbitrary file-read vulnerabilities. These vulnerabilities could allow an attacker to gain remote code execution and read sensitive information to launch more damaging attacks.

**Vulnerable Software Version: MS Remote Desktop (BlueKeep):** Cisco identified a vulnerable version of Microsoft Remote Desktop that was vulnerable to an arbitrary remote code execution vulnerability. This could allow attackers to gain full administrative access to the vulnerable hosts and launch a series of potentially more damaging attacks.

#### High-Risk Findings

**Insecure Software Version: Dropbear SSH Server:** Cisco identified an out-of-date version of Dropbear SSH Server with multiple vulnerabilities. This could allow attackers to gain access to the vulnerable hosts via remote code execution and potentially use the vulnerable system as a pivot point to launch further attacks.

**Insecure Software Version: Dell iDRAC7:** Cisco identified an unsupported version of Dell iDRAC7 that contained many publicly disclosed vulnerabilities, most notably a remote code execution vulnerability. This could allow attackers to gain access to the vulnerable hosts and launch a series of potentially more damaging attacks.

**Insecure Software Version: VMware ESXi:** Cisco identified a vulnerable version of VMWare ESXi with multiple known vulnerabilities, including remote code execution. This could allow attackers to gain access to the vulnerable hosts using publicly available exploits and potentially use the vulnerable system as a pivot point to launch further attacks.

The use of unsupported software was observed:

- MS SQL Server
- PHP
- Windows OS
- OpenSSL

As no further updates/security patches will be released, any affected server will be susceptible to both existing vulnerabilities and any new exploits that might be discovered in the future, allowing an attacker to use publicly available exploits to gain access to a vulnerable host.

#### Medium-Risk Findings

**Insecure Protocol: FTP:** Cisco identified multiple hosts using plain text FTP protocols running on Power Delivery Unit (PDU) devices. This could allow attackers to obtain credentials or data sent over a plain text protocol and could potentially disrupt the operation of hosts powered by the PDU.

**IPMI Protocol Vulnerable To Password Hash Retrieval:** Cisco found that the installed Baseboard Management Controller (BMC) supported management via the Intelligent Platform Management Interface (IPMI) protocol

which was vulnerable to a hash retrieval vulnerability. This could allow attackers to obtain credentials and allow unauthorized control over the hardware, allowing for reboots and other maintenance type activities.

**Insecure Software Version: Apache Tomcat:** Cisco identified an outdated version of Apache Tomcat that was vulnerable to multiple known vulnerabilities. This could allow attackers to gain access to the vulnerable hosts and launch a series of potentially more damaging attacks.

**Insecure Software Version: OpenSSH:** Cisco identified an outdated version of OpenSSH that was vulnerable to multiple known vulnerabilities. If exploited, these vulnerabilities could allow an attacker to potentially gain access to the vulnerable hosts or launch a denial-of-service attack against said hosts.

**Insecure Software Version: Apache:** Cisco identified an outdated and unsupported version of Apache that was vulnerable to multiple known vulnerabilities. As no further updates/security patches will be released, any affected server will be susceptible to both existing vulnerabilities and any new exploits that might be discovered in the future, allowing an attacker to use publicly available exploits to gain access to a vulnerable host.

**libssh Authentication Bypass:** Cisco found a vulnerable version of libssh being used by two (2) vulnerable SSH servers. If exploited, an attacker would be able to gain an SSH session on the vulnerable host and launch a series of potentially more damaging attacks.

**APC InfraStruxure PDU Web Interface Multiple Cross-Site Scripting (XSS) Vulnerabilities:** Cisco identified a vulnerable version of APC InfraStruxure PDU Web Management Interface that was vulnerable to multiple XSS vulnerabilities that could allow an attacker to potentially make changes to the PDU settings and cause a power outage.

**Insecure Protocol: Network Time Protocol (NTP) Mode 6 Scanner:** Cisco identified multiple NTP services that responded to mode 6 queries. This could allow an attacker to launch an NTP amplification attack, creating a reflective denial-of-service condition.

**Network Camera Detection:** Cisco found network cameras that had different views of the data center. This could enable an attacker to either target or keep track of data center employees.

**SSL/TLS Service Uses Expired Certificates:** Cisco found expired certificates in use. Users might become conditioned to ignoring security warnings and could be more likely to fall prey to real attacks.

**Insecure Software Version: NTP:** Cisco found a vulnerable version of NTP in use that was vulnerable to a known denial-of-service vulnerability. This could allow an attacker to put vulnerable hosts out of service.

**SNMP Server Weak Community String Configured:** Cisco found that weak community strings were configured for SNMP services. This could allow an attacker to query the SNMP service to identify security weaknesses in the system configuration.

**Full Firewall Bypass Via IP Over DNS:** Cisco found that the firewall could be bypassed via IP over DNS. This could allow an attacker to exfiltrate data without the limitations of a firewall.

NTP 'Monlist' Command Enabled: Cisco found NTP services that had the 'monlist' command enabled. This could allow an attacker to carry out effective network reconnaissance as the command allows the retrieval of a list of recent hosts that have connected to the service.

SMB Server Does Not Support SMB Packet Signing: Cisco found SMB servers that did not support SMB packet signing. This could allow an attacker to execute a successful "Man-In-The-Middle" attack and potentially gain access to the SMB services.

SNMP 'GETBULK' Reflection Distributed Denial-Of-Service: Cisco found SNMP services vulnerable to a known denial-of-service vulnerability. This could allow an attacker to cause a denial-of-service condition on critical network devices.

Insecure Protocol: Telnet: Cisco found that the Telnet plain text protocol was in use. This could allow an attacker to perform a "Man-In-The-Middle" attack to hijack authenticated sessions and gain access to the vulnerable hosts.

## STRENGTHS

Some default passwords were changed.

Most web services have a permanent redirection from the application served on HTTP to HTTPS for secure transport.

## WEAKNESSES

### Weak Password Requirements

#### DESCRIPTION

The password policy is insufficient to ensure that appropriately secure passwords are set.

#### SOLUTION

Ensure that all accounts have a strong password set. Passwords should have an appropriate complexity based on the type and level of access and the systems on which they can be used. Each password should be created from a large character set that forces the user to select a combination of upper, lower and special case characters as well as numbers. In addition, they should not be based on a dictionary word, the username or the associated system.

## Missing Security Patches

### DESCRIPTION

Missing security patches indicate an insufficient patching policy, which could result in a compromise of the environment assessed.

### SOLUTION

Apply all missing patches, and review current procedures to ensure that security patches are applied to all relevant systems in a timely manner going forward.

## Insecure Configuration

### DESCRIPTION

Insecure configuration can lead to sensitive information being disclosed or services being exposed to attack.

### SOLUTION

Modify the current configuration files to ensure they adhere to good practice principles, and conduct regular configuration reviews to ensure that current variables are up-to-date with the latest industry good security practice guidelines.

## Improper Validation of Certificate - Expiration

### DESCRIPTION

Out-of-date certificates cause warning messages to appear in browsers. Users can become conditioned to accepting these, which could lead to them ignoring a warning about a 'Man-In-The-Middle' attack.

### SOLUTION

Ensure that all SSL/TLS certificates are up-to-date and not due to expire in the immediate future. Ensure that all certificates are renewed in good time.

## Information Exposure

### DESCRIPTION

Information exposure is the intentional or unintentional disclosure of information to any party not explicitly authorised to have access to it.

### SOLUTION

All unnecessary content should be removed from the application or sufficiently obscured.



## Transmission of Sensitive Information In Plain Text

### DESCRIPTION

Data passed between the client and server is not encrypted, potentially exposing sensitive data that could be intercepted by an attacker able to obtain access to the affected network segment.

### SOLUTION

Sensitive data should always only ever be transmitted securely. Unencrypted protocols should be replaced with encrypted alternatives wherever possible.

## INDEX OF FINDINGS

Finding Title	Severity Rating	CVSS Score
1. Default Password In Use: Dell iDRAC	CRITICAL	9.9
2. Default Passwords Present On Server	CRITICAL	9.8
3. Public Git Repositories Available Expose Sensitive Information	CRITICAL	9.8
4. Insecure Software Version: VMware VCenter Server	CRITICAL	9.3
5. Vulnerable Software Version: MS Remote Desktop (BlueKeep)	CRITICAL	9.1
6. Insecure Software Version: Dropbear SSH Server	HIGH	8.5
7. Insecure Software Version: Dell iDRAC7	HIGH	8.3
8. Insecure Software Version: VMware ESXi	HIGH	7.5
9. Insecure Software Version: MS SQL Server Version Unsupported	HIGH	7.3
10. Insecure Software Version: PHP Unsupported	HIGH	7.3
11. Insecure Software Version: Windows OS Unsupported	HIGH	7.3
12. Insecure Software: OpenSSL Unsupported	HIGH	7.3
13. Insecure Protocol: FTP	MEDIUM	6.8
14. IPMI Protocol Vulnerable To Password Hash Retrieval	MEDIUM	6.7
15. Insecure Software Version: Apache Tomcat	MEDIUM	6.5
16. Insecure Software Version: OpenSSH	MEDIUM	6.5
17. Insecure Software Version: Apache	MEDIUM	6.4
18. libssh Authentication Bypass	MEDIUM	6.2
19. APC InfraStruxure PDU Web Interface Multiple Cross-Site Scripting (XSS) Vulnerabilities	MEDIUM	5.9
20. Insecure Protocol: Network Time Protocol (NTP) Mode 6 Scanner	MEDIUM	5.3
21. Network Camera Detection	MEDIUM	5.3



Finding Title	Severity Rating	CVSS Score
22. SSL/TLS Service Uses Expired Certificates	MEDIUM	5.3
23. Insecure Software Version: NTP	MEDIUM	5.2
24. SNMP Server Weak Community String Configured	MEDIUM	5.1
25. Full Firewall Bypass Via IP Over DNS	MEDIUM	4.9
26. NTP 'Monlist' Command Enabled	MEDIUM	4.8
27. SMB Server Does Not Support SMB Packet Signing	MEDIUM	4.6
28. SNMP 'GETBULK' Reflection Distributed Denial Of Service	MEDIUM	4.6
29. Insecure Protocol: Telnet	MEDIUM	4.2

## 4. Internal Infrastructure Assessment

### 4.1. Default Password In Use: Dell iDRAC

Severity Rating	CRITICAL	CVSS Score	9.9
CWE Category	CWE-521: Weak Password Requirements		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified the use of a default password on one Dell iDRAC server. This password permitted administrator-level login and console access, shown in the screenshots below:

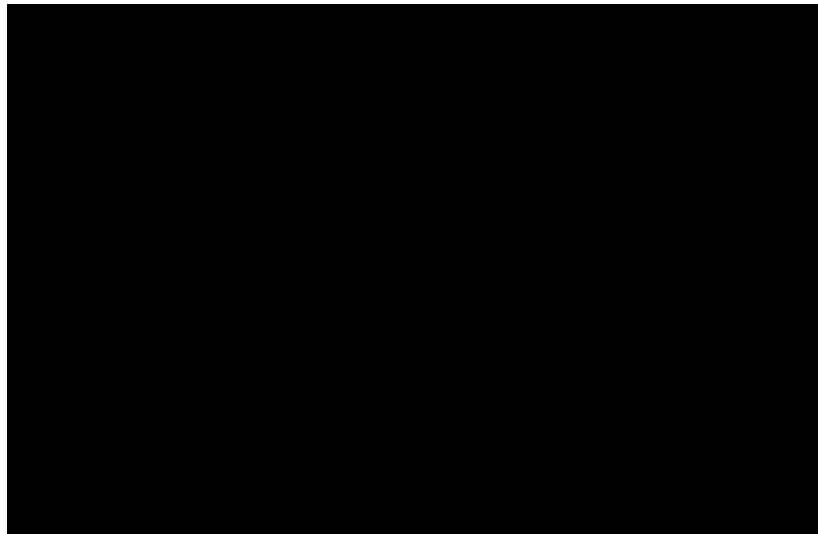
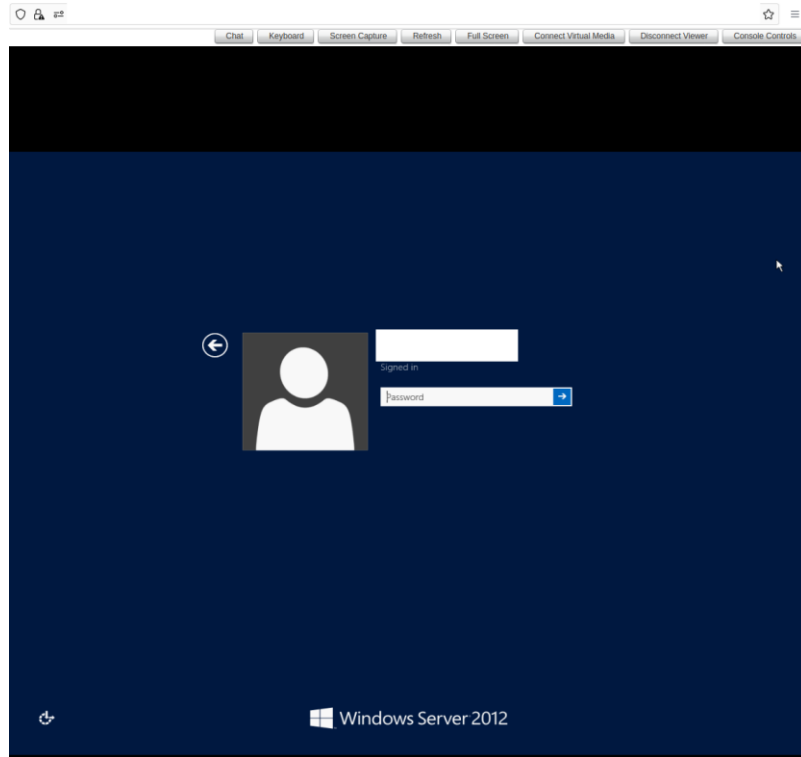


Figure 1 - An Image Showing Authenticating As Root Provides Access To User List



*Figure 2 - An Image Showing Access To System Console Using iDRAC Default Credentials*

### Impact

Allowing weak and predictable user passwords presents a significant security risk as it renders the associated accounts vulnerable to brute-force and/or password guessing attacks. After compromising a user account, the successful attacker could exploit the account's permissions, potentially leading to a series of more damaging attacks. As the affected host is a Dell iDRAC unit, an attacker might disrupt operation of potentially critical systems.

### Recommendation

Cisco recommends setting strong passwords for any identified accounts, keeping in mind that the underlying IPMI protocol exposes password hashes that might be cracked offline.

## 4.2. Default Passwords Present On Server

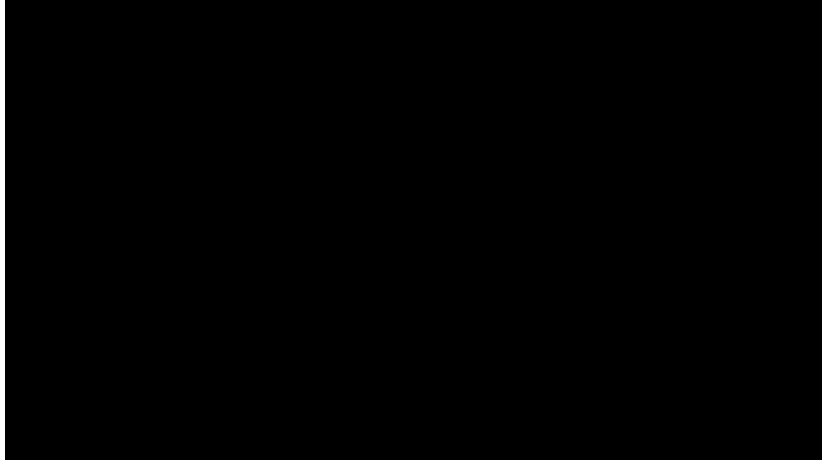
Severity Rating	<b>CRITICAL</b>	CVSS Score	<b>9.8</b>
CWE Category	CWE-521: Weak Password Requirements		
Affected Components	Please see appendix for a full list of all 23 affected components - <a href="#">Full List</a>		

### Specific Detail

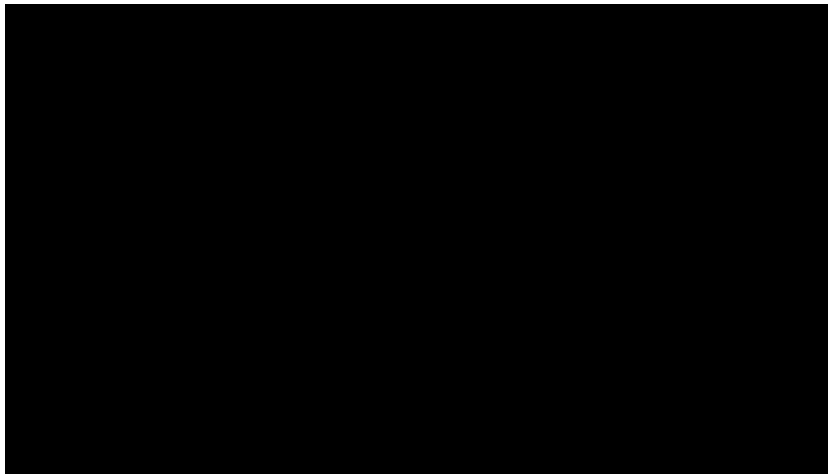
The Team discovered known default credentials that were being used. The following passwords were found to be valid:

- REDACTED
- REDACTED

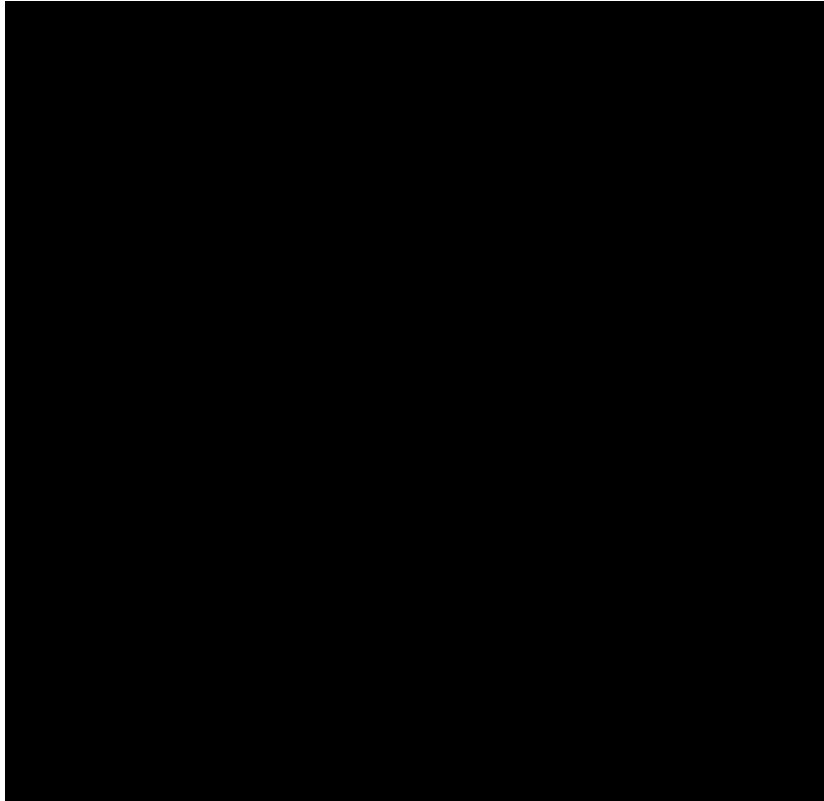
Host	Username



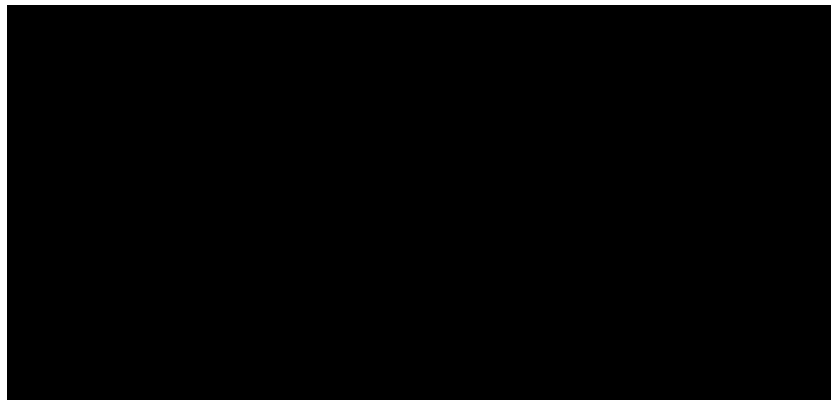
*Figure 3 - An Image Showing Successful Login Via SSH To One Endura CCTV Recorder Host*



*Figure 4 - An Image Showing Successful Retrieval Of Password Of Endura CCTV Recorder Web Management Interface*



*Figure 5 – An Image Showing Endura CCTV Recorder Web Management Interface After Successfully Logging In*



*Figure 6 – An Image Showing Successful Login Via SSH To One APC InfraStruxure PDU Host*

#### Impact

Allowing weak and predictable user passwords presents a significant security risk as it renders the associated accounts vulnerable to brute-force and/or password guessing attacks. After compromising a user account, the successful attacker could exploit the account's permissions, potentially leading to a series of more damaging attacks.



## Recommendation

Cisco recommends auditing systems on a regular basis for the presence of weak passwords, and that an appropriate password policy consisting of a defined set of rules is put in place (if not already present). Where password policy changes have been retrospectively applied to a system, all account passwords should be forcibly changed to comply with the new policy.

Good practice dictates that passwords should:

- Be a minimum of nine characters in length
- Consist of a mix of upper and lower case characters, at least one number and at least one non-alphanumeric character
- Not contain the username or application name
- Not be based on a dictionary word
- Not be the default password

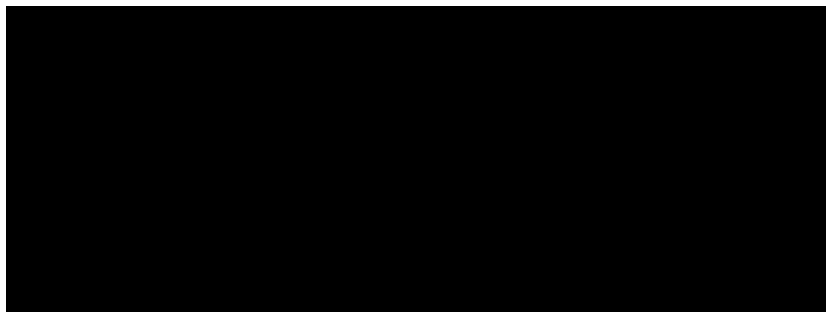
Note: Simply adding a few numbers as a prefix and/or suffix to words does not constitute effective protection, either online or offline.

### 4.3. Public Git Repositories Available Expose Sensitive Information

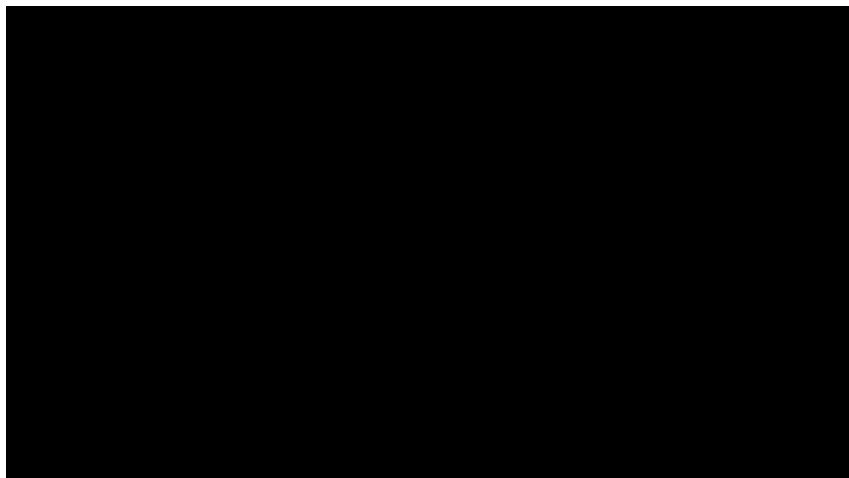
Severity Rating	CRITICAL	CVSS Score	9.8
CWE Category	CWE-552: Files or Directories Accessible to External Parties		
Affected Components	[REDACTED]		

#### Specific Detail

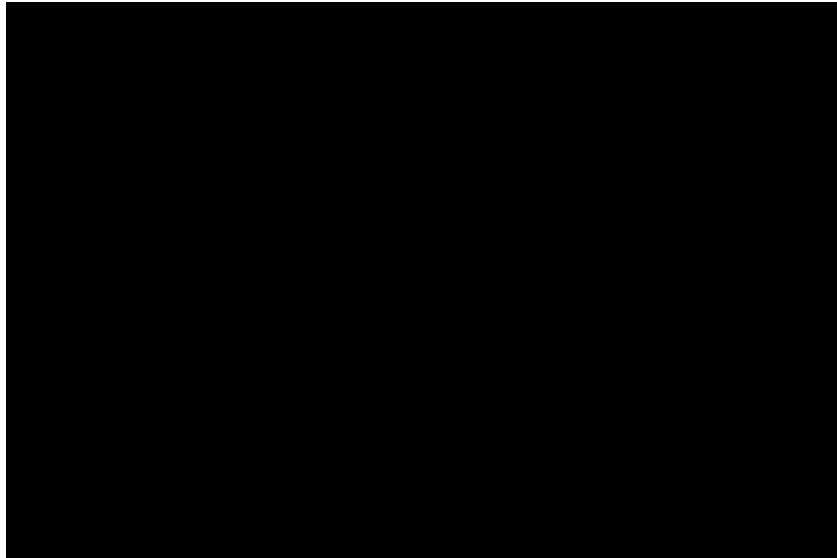
The Team identified that Git repositories were available on the affected web servers. Users did not need to log in to view the repositories. The repositories contained sensitive information such as rolling backup configuration files for network devices in the organization that included secret hashes, usernames, hostnames, etc.



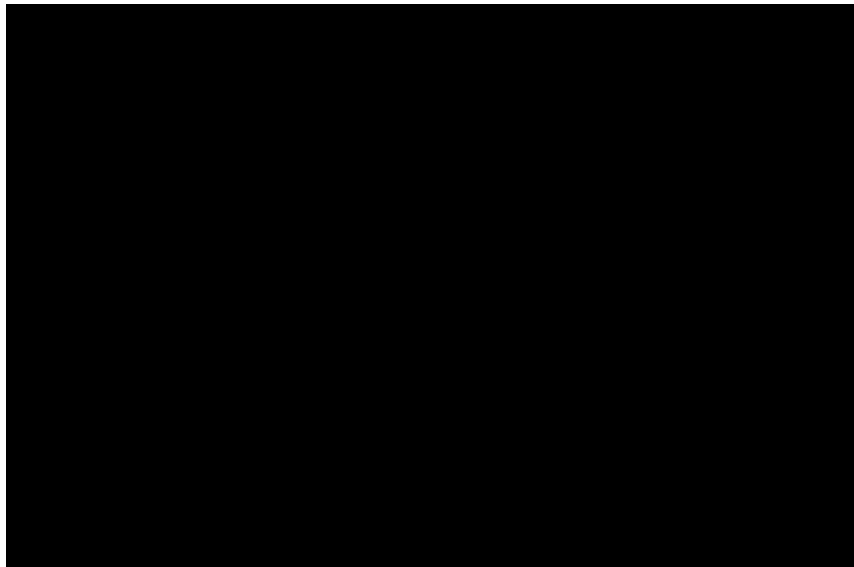
*Figure 7 – An Image Showing Rolling Backups Public Repository*



*Figure 8 – An Image Showing Ansible Playbooks Public Repository*



*Figure 9 – An Image Showing Recent Backup Of Configuration File Of Cisco Device Including Secret Hash*



*Figure 10 – An Image Showing Encrypted Content In One Of The Ansible Repositories*

### General Background

Version control repositories such as CVS or Git store version-specific metadata and other details within subdirectories. If these subdirectories are stored on a web server or added to an archive, then these could be used by an attacker. This information might include usernames, filenames, path root, IP addresses, and detailed "diff" data about how files have been changed - which could reveal source code snippets that were never intended to be made public.

### Impact

An attacker could download the contents of the Git repository, which included sensitive information like network device configuration files.

### Recommendation

Cisco recommends removing the Git repository from the server, or only exposing it to a limited number of users, rather than configuring it as a public repository. This can be done by setting the repository to private in settings and granting only necessary users roles for the repository to both limit access and follow the principle of least privileges.

#### 4.4. Insecure Software Version: VMware vCenter Server

Severity Rating	<b>CRITICAL</b>	CVSS Score	<b>9.3</b>
CWE Category	CWE-671: Lack of Administrator Control over Security		
Affected Components	[REDACTED]		

#### Specific Detail

The Team observed one (1) outdated version of VMware vCenter Server, containing known vulnerabilities that permit code execution and information disclosure. Please refer to the following CVE reports for additional information:

- CVE-2021-22049
- CVE-2021-21980

Component	Details
[REDACTED]	Installed version : 6.7 Build x

#### Impact

An attacker who exploits the known vulnerabilities on this platform might gain significant control within vCenter, potentially compromising data and availability.

#### Recommendation

Cisco recommends upgrading to the most recent supported version of VMware vCenter. Please see <https://kb.vmware.com/s/article/2143838> for additional information about vCenter Server versions.

#### 4.5. Vulnerable Software Version: MS Remote Desktop (BlueKeep)

Severity Rating	CRITICAL	CVSS Score	9.1
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team discovered that a critical Microsoft patch had not been applied to the Remote Desktop Protocol (RDP) service. The Team was able to exploit this vulnerability to gain administrative account access on the vulnerable hosts.

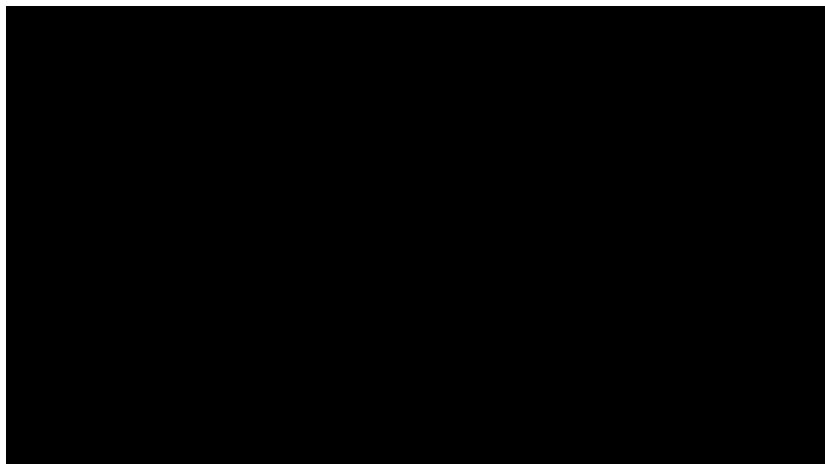
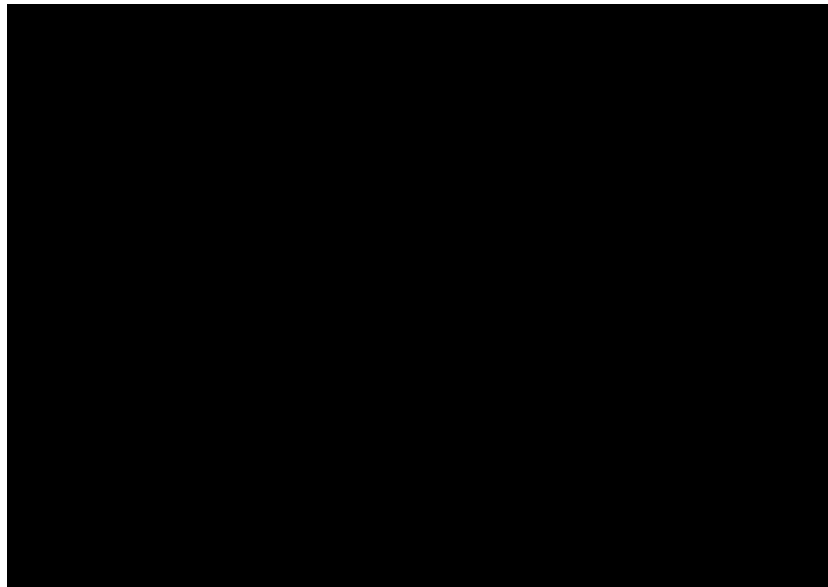


Figure 11 – An Image Showing Launching Of A Metasploit Module



*Figure 12 – An Image Showing Successful Connection To Bind Shell Launched As Administrative User*

#### General Background

A vulnerability in the Remote Desktop Services component of Microsoft Windows could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system.

The vulnerability exists as the affected software improperly handles Remote Desktop Protocol (RDP) requests. An attacker could exploit the vulnerability by sending RDP connection requests that submit malicious input to the affected software.

#### Impact

An attacker could exploit the vulnerability by sending RDP connection requests that submit malicious input to the affected software. A successful exploit could allow the attacker to execute arbitrary code and completely compromise the system.

#### Recommendation

Cisco recommends applying the proper security update(s) from Microsoft for the affected system version(s). Refer to the following links for more information:

- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>
- <https://www.microsoft.com/security/blog/2019/08/08/protect-against-bluekeep/>

#### 4.6. Insecure Software Version: Dropbear SSH Server

Severity Rating	<b>HIGH</b>	CVSS Score	<b>8.5</b>
CWE Category	CWE-0: Missing Security Patches		
Affected Components	<div style="background-color: black; width: 100%; height: 1.2em; margin-bottom: 2px;"></div> <div style="background-color: black; width: 100%; height: 1.2em; margin-bottom: 2px;"></div> <div style="background-color: black; width: 100%; height: 1.2em; margin-bottom: 2px;"></div>		

#### Specific Detail

The Team identified that the version of Dropbear SSH Server was out-of-date and susceptible to four (4) known vulnerabilities.

These four vulnerabilities are:

- Improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges (CVE-2016-7406)
- Insecure handling of specially crafted OpenSSH key files in dropbearconvert. An unauthenticated, remote attacker can exploit this to execute arbitrary code (CVE-2016-7407)
- A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code (CVE-2016-7408)
- If dbclient or dropbear server are compiled with the DEBUG\_TRACE option and then run using the -v switch, an attacker with local access to the operating system can exploit this to disclose process memory (CVE-2016-7409)

All affected hosts indicated the following:

```
Version source      : SSH-2.0-dropbear_2014.66
Fixed version      : 2016.74
```

#### Impact

The vulnerabilities that this version of Dropbear SSH is susceptible to can lead to system compromise via arbitrary code execution or disclosure of sensitive information in memory, such as authentication credentials.



## Recommendation

Cisco recommends upgrading the Dropbear SSH server to the latest version.

- <https://matt.ucc.asn.au/dropbear/CHANGES>

#### 4.7. Insecure Software Version: Dell iDRAC7

Severity Rating	HIGH	CVSS Score	8.3
CWE Category	CWE-671: Lack of Administrator Control over Security		
Affected Components	██████████		

#### Specific Detail

The Team identified one (1) Dell iDRAC7 running an old firmware version. iDRAC7 has reached end of software maintenance as of February, 2020, and the vendor is no longer issuing security updates.

Please refer to <https://www.dell.com/support/kbdoc/en-us/000175831/support-for-integrated-dell-remote-access-controller-7-iDRAC7> for more information.

Known vulnerabilities in this version include Privilege Escalation, Buffer Overflow, Code Execution, and Information Disclosure. Please refer to the following CVE reports for additional information:

- CVE-2018-1000116
- CVE-2018-1207
- CVE-2018-1211
- CVE-2018-1212
- CVE-2018-1243
- CVE-2018-1244
- CVE-2018-1249
- CVE-2018-15774
- CVE-2018-15776
- CVE-2020-5344

#### Impact

A successful attacker might disrupt operation of potentially critical systems.



## Recommendation

Cisco recommends upgrading the iDRAC7 platform to a supported version. Alternatively, Cisco recommends moving the server to a dedicated network segment with network level access controls that deny unauthenticated and unauthorized access.

#### 4.8. Insecure Software Version: VMware ESXi

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.5</b>																								
CWE Category	CWE-0: Missing Security Patches																										
Affected Components	<table border="1"> <tr> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> </tr> <tr> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> </tr> <tr> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> <td>██████████</td> </tr> <tr> <td>████████████████████</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>			██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	██████████	████████████████████					
██████████	██████████	██████████	██████████	██████████	██████████																						
██████████	██████████	██████████	██████████	██████████	██████████																						
██████████	██████████	██████████	██████████	██████████	██████████																						
████████████████████																											

#### Specific Detail

The Team discovered that the version of VMWare ESXi in use was out-of-date and potentially contained known/documented vulnerabilities. The hosts and versions shown below were identified as out-of-date and contained one or more known vulnerabilities.

Please refer to the following CVE reports for addition information:

- CVE-2020-4004 - Code Execution
- CVE-2020-4005 - Privilege Escalation
- CVE-2021-22040 - Code Execution
- CVE-2021-22041 - Code Execution
- CVE-2021-22042 - Unauthorized Access
- CVE-2021-22043 - Privilege Escalation
- CVE-2021-22050 - Denial of Service

Component	Details
████████████████████	ESXi version : 6.7 Installed build : 17700523 Fixed build : 18828794
████████████████████	ESXi version : 6.7 Installed build : 17700523 Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 16713306  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 17700523  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 16713306  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 16713306  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 17700523  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 17700523  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 17700523  
Fixed build : 18828794

[REDACTED]

ESXi version : 6.7  
Installed build : 17700523  
Fixed build : 18828794

## Impact

Running out-of-date services can expose a wide range of vulnerabilities, from simple information disclosure through to serious attacks such as Denial-of-Service and remote code execution (RCE).

Successful exploitation might give the attacker broad access to the affected host.

Generally, software that is not up-to-date poses a significant risk to any environment because vendors frequently release software updates that address security vulnerabilities in the software.

## Recommendation

Cisco recommends patching the affected hosts to current and supported versions of VMware ESXi.

#### 4.9. Insecure Software Version: MS SQL Server Version Unsupported

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.3</b>
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team observed the following obsolete server version details (i.e., where the vendor or provider no longer supports the particular version).

Component	Details
[REDACTED]	<p>The following unsupported installation of Microsoft SQL Server was detected:</p> <ul style="list-style-type: none"> <li>• Installed version : 11.0.2100.0</li> <li>• Latest version : 11.0.7001.0 (2012 SP4)</li> <li>• SQL Server Instance : EXEMPLUM_DB</li> </ul>

#### Impact

As no further updates/security patches will be released, any affected server will be susceptible to both existing vulnerabilities and any new exploits that may be discovered in the future. In either case, an attacker may be able to use publicly available exploits to potentially gain control of any machine running an obsolete version.

It should be noted that while there may be less research aimed at finding new vulnerabilities in the obsolete version in use, and that a potential attacker may have to rely on the exploit code currently available, this should not be taken as grounds for complacency in terms of the ongoing security of the service.

#### Recommendation

Cisco recommends replacing the Microsoft SQL server with a version that is currently supported by Microsoft. Details of currently supported Windows operating systems can be found on the Microsoft website.

#### 4.10. Insecure Software Version: PHP Unsupported

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.3</b>
CWE Category	CWE-671: Lack of Administrator Control over Security		
Affected Components	[REDACTED]		

#### Specific Detail

The Team reported the following out-of-date PHP version details (which indicated that the system was vulnerable to multiple issues). The installed version identified is 5.2.6 and 7.2.7, which are now beyond end-of-life (EOL).

Component	Details
[REDACTED]	Server: X-Powered-By: PHP/7.2.7 Installed version: 7.2.7 End of support date: 2020/11/30 Announcement: <a href="http://php.net/supported-versions.php">http://php.net/supported-versions.php</a> Supported versions: 7.3.x / 7.4.x / 8.0.x
[REDACTED]	Server: X-Powered-By: PHP/7.2.7 Installed version: 7.2.7 End of support date: 2020/11/30 Announcement: <a href="http://php.net/supported-versions.php">http://php.net/supported-versions.php</a> Supported versions: 7.3.x / 7.4.x / 8.0.x
[REDACTED]	Server: Server: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.8e DAV/2 PHP/5.2.6 Installed version: 5.2.6 End of support date: 2011/01/06 Announcement: <a href="http://php.net/eol.php">http://php.net/eol.php</a>



Supported versions : 7.3.x / 7.4.x / 8.0.x

Server: Apache/2.2.9 (Unix) mod\_ssl/2.2.9 OpenSSL/0.9.8e DAV/2 PHP/5.2.6

Installed version: 5.2.6

End of support date: 2011/01/06

Announcement: <http://php.net/eol.php>

Supported versions: 7.3.x / 7.4.x / 8.0.x

## Impact

Running an out-of-date version of PHP potentially exposes the system to security issues across the following categories:

- Input Sanitization
- Cross-site Scripting
- Heap Overflow
- Buffer Overflow
- Denial of Service
- Information Disclosure
- “Man-In-The-Middle”
- Unexpected Uploads
- Session Corruption
- Arbitrary URL Redirection

An unsupported version of PHP will not have security patches released when issues are identified. As no more updates/security patches will be released, any affected service will be susceptible to both existing vulnerabilities and any new exploits that might be discovered in the future. In either case, an attacker might be able to use publicly available exploits to potentially gain control of any machine running an obsolete version.

## Recommendation

Cisco recommends upgrading PHP to the latest software version.

In addition, policies and procedures should be introduced (or existing ones reviewed) to ensure that all new security patches are applied as soon as they become available.

#### 4.11. Insecure Software Version: Windows OS Unsupported

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.3</b>
CWE Category	CWE-0: Missing Security Patches		
Affected Components	██████████		

#### Specific Detail

The Team observed the following obsolete server version details (i.e., where the vendor or provider no longer supports the particular version):

Component	Details
██████████	<p>The following Windows version is installed and not supported:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 7 Ultimate</li> </ul>

#### General Background

For additional information on Microsoft OS support, please see:

- <https://support.microsoft.com/en-us/hub/4095338/microsoft-lifecycle-policy>

#### Impact

As no further updates/security patches will be released, any affected server will be susceptible to both existing vulnerabilities and any new exploits that may be discovered in the future. In either case, an attacker may be able to use publicly available exploits to potentially gain control of any machine running an obsolete version.

It should be noted that while there may be less research aimed at finding new vulnerabilities in the obsolete version in use, and that a potential attacker may have to rely on the exploit code currently available, this should not be taken as grounds for complacency in terms of the ongoing security of the service.

#### Recommendation

Cisco recommends that the Microsoft Windows 7 operating system be replaced with a version of Windows currently supported by Microsoft. Details of currently supported Windows operating systems can be found on the Microsoft website.

#### 4.12. Insecure Software: OpenSSL Unsupported

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.3</b>
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team discovered OpenSSL versions 0.9.8e to be in use. This version of OpenSSL is no longer supported, which implies that no new security patches for the product will be released by the vendor.

Component	Details
[REDACTED]	Reported version : 0.9.8e See: <a href="https://www.openssl.org/policies/releasestrat.html">https://www.openssl.org/policies/releasestrat.html</a>
[REDACTED]	Reported version : 0.9.8e See: <a href="https://www.openssl.org/policies/releasestrat.html">https://www.openssl.org/policies/releasestrat.html</a>

#### General Background

According to its banner, the remote web server uses a version of OpenSSL that is no longer supported, which implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See also:

- <https://www.openssl.org/news/openssl-old-notes.html>

#### Impact

No more updates/security patches will be released for this software; therefore, it could be susceptible to both existing vulnerabilities that remain unpatched and new exploits that may be discovered in the future. In either case, an attacker might be able to use publicly-available exploits to potentially gain control of any machine running this system.



Note: While there might be less research aimed at finding new vulnerabilities in this obsolete version and that a potential attacker might have to rely on the exploit code currently available, this should not be taken as grounds for complacency in terms of the ongoing security of the platform.

#### Recommendation

Cisco recommends an upgrade to a supported version of OpenSSL: <https://www.openssl.org/source/>.

### 4.13. Insecure Protocol: FTP

Severity Rating	MEDIUM	CVSS Score	6.8
CWE Category	CWE-0: Use Of Insecure Protocols		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified plain text FTP servers operating on seven (7) APC PDU devices.

#### General Background

Plain text protocols might be captured while in transit, then decoded in order to recover session contents. Credentials exchanged by these protocols can be captured and replayed indefinitely until they are changed or invalidated.

#### Impact

An attacker who obtains credentials for an APC PDU might be able to affect the operation of the PDU and potentially disrupt the operation of hosts and infrastructure powered by the PDU.

#### Mitigating Factors

The attacker must have access to data in transit between the FTP server and the FTP client.

#### Recommendation

Cisco recommends migrating insecure protocols to secure alternatives. SFTP or SSH could provide suitable, secure file transfer functionality.

#### 4.14. IPMI Protocol Vulnerable To Password Hash Retrieval

Severity Rating	MEDIUM	CVSS Score	6.7
CWE Category	CWE-201: Information Exposure Through Sent Data		
Affected Components	Please see appendix for a full list of all 11 affected components - <a href="#">Full List</a>		

#### Specific Detail

The Team observed that the installed Baseboard Management Controller (BMC) supported management via the Intelligent Platform Management Interface (IPMI) protocol, which is susceptible to a hash retrieval vulnerability.

The IPMI protocol contains a number of flaws, one of which is that the protocol stipulates that the server sends a salted SHA1 or MD5 hash of the password to the client before authentication, potentially enabling the retrieval of the password hash for any known user on the BMC (typically, most BMCs ship with a number of well-known default users).

The following screenshot demonstrates recovery of IPMI password hashes on the affected hosts:

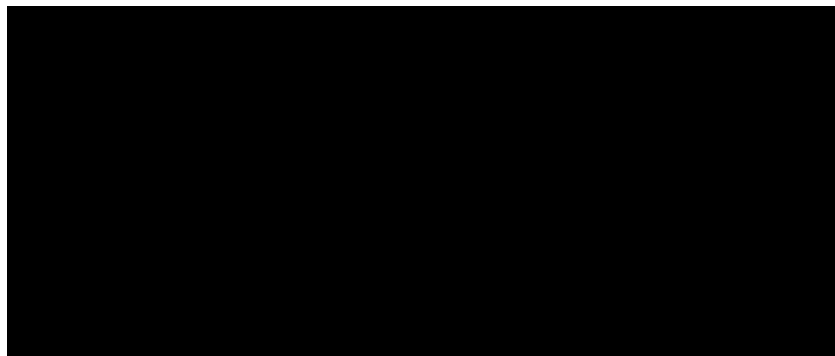


Figure 13 – An Image Showing Use Of Metasploit Framework To Recover IPMI Password Hashes

#### Impact

At a minimum, availability of the hash value enables offline password cracking, while in the worst case, a weak password is rapidly discovered and then exploited.

Unauthorized access to the BMC will generally allow control over the hardware, allowing for reboots and other maintenance type activities and, in some circumstances, access to the core operating system on the affected host might be possible.

## Recommendation

Cisco recommends that, if possible, either the IPMI protocol is disabled or that access restrictions are put in place to allow access from trusted hosts only. Where this is not possible, all default users should be changed, and strong passwords set to protect against the easy retrieval and cracking of password hashes.

## Steps to Replicate

Metasploit is the easiest way to extract the IPMI hashes:

```
msf> use auxiliary/scanner/ipmi/ipmi_dumphashes
msf auxiliary(ipmi_dumphashes) > set RHOSTS 192.168.91.0/24
msf auxiliary(ipmi_dumphashes) > set THREADS 16
msf auxiliary(ipmi_dumphashes) > run
```

#### 4.15. Insecure Software Version: Apache Tomcat

Severity Rating	MEDIUM	CVSS Score	6.5
CWE Category	CWE-671: Lack of Administrator Control over Security		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified one (1) outdated Apache Tomcat installation, version 8.0.30, with support having ended in June 2018. This version contains multiple known vulnerabilities, including Denial of Service, Code Execution, Access Control Bypass, Information Disclosure, Cross-Site Request Forgery, and Cross-Site Scripting.

Please refer to the following CVE reports for additional details:

- CVE-2015-5346
- CVE-2015-5351
- CVE-2016-0706
- CVE-2016-0714
- CVE-2016-0762
- CVE-2016-0763
- CVE-2016-3092
- CVE-2016-5018
- CVE-2016-6794
- CVE-2016-6796
- CVE-2016-6797
- CVE-2016-6816
- CVE-2016-6817
- CVE-2016-8735
- CVE-2016-8745
- CVE-2017-12617
- CVE-2017-5647
- CVE-2017-5648
- CVE-2017-5664
- CVE-2017-7674
- CVE-2018-1304
- CVE-2018-1305
- CVE-2018-1336
- CVE-2018-8014
- CVE-2018-8034



Component	Details
████████████████████	Installed version : 8.0.30 Support ended : 2018-06-30 Additional information : <a href="http://tomcat.apache.org/tomcat-80-eol.html">http://tomcat.apache.org/tomcat-80-eol.html</a>

### Impact

An attacker might gain access to the server platform, resulting in compromise of the server, along with its data and functionality. If the server contains credentials for services elsewhere, an attacker could use those to attack those other services.

As no further updates/security patches will be released, any affected server will be susceptible to both existing vulnerabilities and any new exploits that might be discovered in the future. In either case, an attacker might be able to use publicly available exploits to potentially gain control of any machine running an obsolete version.

Note: While there might be less research aimed at finding new vulnerabilities in the obsolete version in use, and that a potential attacker might have to rely on the exploit code currently available, this should not be taken as grounds for complacency in terms of the ongoing security of the service.

### Recommendation

Cisco recommends upgrading to the most current and supported release of Apache Tomcat. Please refer to <https://tomcat.apache.org/> for information about current releases.

#### 4.16. Insecure Software Version: OpenSSH

Severity Rating	MEDIUM	CVSS Score	6.5
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team observed two (2) outdated OpenSSH servers containing known vulnerabilities, including Plain text Disclosure, Session Hijacking, Denial of Service, and Authentication Bypass. Please refer to the following CVE reports for more information:

- CVE-2008-1483
- CVE-2008-3234
- CVE-2008-3259
- CVE-2008-5161
- CVE-2011-4327

Component	Details
[REDACTED]	Version source : SSH-2.0-OpenSSH_4.9 Installed version : 4.9
[REDACTED]	Version source : SSH-2.0-OpenSSH_4.9 Installed version : 4.9

#### Impact

A successful exploit might yield shell access to the affected hosts, allowing the attacker to access data and functionality associated with the compromised session or account.

## Recommendation

Cisco recommends upgrading to the most recent and supported version of OpenSSH, currently at Version 9.

Note: Version 8 and its point releases might allow an attacker to alter version negotiation and gain a foothold into the SSH session.

#### 4.17. Insecure Software Version: Apache

Severity Rating	MEDIUM	CVSS Score	6.4
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified that the version of Apache web server in use was out-of-date by several revisions and, depending on how it was compiled, might be susceptible to multiple vulnerabilities.

Please refer to the following notice at <https://httpd.apache.org/> explaining the end of life of Apache web server version 2.2 as of June 2017.

Please refer to the following CVE reports for additional information about vulnerabilities in Apache web server version 2.2.9. This list is extensive and encompasses a range of vulnerability classes.

- CVE-2007-6750
- CVE-2009-0023
- CVE-2009-1191
- CVE-2009-1195
- CVE-2009-1890
- CVE-2009-1891
- CVE-2009-1955
- CVE-2009-1956
- CVE-2009-2412
- CVE-2009-2699
- CVE-2009-3094
- CVE-2009-3095
- CVE-2009-3555
- CVE-2009-3560
- CVE-2009-3720
- CVE-2010-0408
- CVE-2010-0425
- CVE-2010-0434
- CVE-2010-1452
- CVE-2010-1623
- CVE-2010-2068
- CVE-2011-0419
- CVE-2011-3348
- CVE-2011-3368
- CVE-2011-3607
- CVE-2011-4317
- CVE-2012-0021
- CVE-2012-0031
- CVE-2012-0053
- CVE-2012-0883
- CVE-2012-2687
- CVE-2012-3499
- CVE-2012-4557
- CVE-2012-4558
- CVE-2013-1862
- CVE-2013-1896
- CVE-2013-5704
- CVE-2013-6438
- CVE-2014-0098
- CVE-2014-0118
- CVE-2014-0226
- CVE-2014-0231
- CVE-2017-3167
- CVE-2017-3167
- CVE-2017-3169



- CVE-2017-3169
- CVE-2017-7659
- CVE-2017-7668
- CVE-2017-7668
- CVE-2017-7679
- CVE-2017-7679
- CVE-2017-9788
- CVE-2021-34798
- CVE-2021-39275
- CVE-2021-40438
- CVE-2022-22719
- CVE-2022-22720
- CVE-2022-22721
- CVE-2022-23943

Component	Details
██████████ ██████████	Version source : Server: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.8e DAV/2 PHP/5.2.6  Installed version : 2.2.9
██████████ ██████████	Version source : Server: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.8e DAV/2 PHP/5.2.6  Installed version : 2.2.9

### Impact

Newer versions of software become available over time as patches are released to fix known vulnerabilities. These are often published with exploit code.

### Recommendation

Cisco recommends that the version of Apache is upgraded to the latest available version. In addition, policy and procedure should be reviewed to ensure that the software is kept up-to-date with the latest security patches, going forward.

Specific information about current and supported versions of the Apache web server are available at <https://httpd.apache.org>.

#### 4.18. libssh Authentication Bypass

Severity Rating	MEDIUM	CVSS Score	6.2
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team established a session on two (2) vulnerable SSH servers that utilize an outdated version of libssh.

Please refer to the following CVE reports for additional information:

- CVE-2018-10933
- CVE-2018-1000805

#### Impact

An attacker might use an SSH session to further exploit the host system, its data, and its functionality.

#### Recommendation

Cisco recommends upgrading to the most recent and supported version of libssh. For more information, please refer to <https://www.libssh.org/>.

#### 4.19. APC InfraStruxure PDU Web Interface Multiple Cross-Site Scripting (XSS) Vulnerabilities

Severity Rating	MEDIUM	CVSS Score	5.9
CWE Category	CWE-79: Improper Neutralisation of Input During Web Page Generation (Cross-site Scripting)		
Affected Components	[REDACTED]		

#### Specific Detail

The Team discovered that the APC InfraStruxure PDU Network Management Card web instance was vulnerable to multiple reflected Cross-Site Scripting (XSS) vulnerabilities (CVE-2021-22812 and CVE-2021-22810). The issues were first found in NMC2 AOS versions 6.9.6 and below and have not yet been officially patched. However, the version of NMC2 AOS running on the affected hosts was found to be version 5.1.9.



Figure 14 – An Image Showing System Information Returned By APC InfraStruxure PDU Shell That Includes Version

In the case of the current web application, the XSS was "reflected", meaning that a user would need to follow a specially crafted link for the attack to be successful.

## General Background

In 2021, multiple XSS vulnerabilities were discovered in APC by Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices. Cross-Site scripting (XSS) occurs when HTTP responses generated by the application include user input that has not been appropriately encoded. The semantics of these responses can be altered by including HTML metacharacters in user supplied input, such as the less-than symbol, greater-than symbol, and single and double quotes.

A browser interprets these characters in an affected response instead of rendering them, resulting in conditions where an attacker can execute arbitrary JavaScript in the browser of another user or alter the HTML display in some advantageous way (e.g., fake login form or site defacement). Additionally, if the user supplied input is placed directly inside of a script code block, no HTML metacharacters are required to exploit the vulnerability.

In cases where user supplied input parameters are stored and then later find their way into HTTP responses, the attack is called stored Cross-Site Scripting. In cases where an HTTP request parameter is echoed in the corresponding HTTP response, the attack is known as reflected Cross-Site Scripting.

Common attacks using Cross-Site Scripting vulnerabilities involve luring a user to a page containing malicious JavaScript that will execute in the security context of the target web site. This allows the malicious script to perform restricted operations and provides an attacker with access to sensitive information stored in the target user's browser, typically session cookies. Additionally, requests within the site can be automated and performed on the target user's behalf.

## Impact

A successful attack might permit changes to PDU settings that can disrupt the operation of hosts and infrastructure. An attacker could achieve this by exploiting this flaw to get active HTML or script code executed in an authenticated user's browser. Cross-Site Scripting might be used to perform attacks such as session hijacking by invoking the user's browser to send information stored in their cookies (such as a session identification token) to an arbitrary location controlled by the attacker. Furnished with this information, the attacker could immediately access the site, masquerading as the authenticated user who viewed the page containing the malicious code. The attacker would then be able to perform actions as the authorized user, subject to their role, which could include viewing sensitive data, modifying profile information and making transactions.

Additionally, an attacker could use Cross-Site Scripting to exploit vulnerabilities within web browsers. The outcome of such an attack would depend on the exploits used, but in a worst case scenario, the attacker could gain full control of a user's computer. Once that had been achieved, it would be trivial for the attacker to



install a keystroke logger and gain access to applications via the usernames and passwords they had acquired.

#### Mitigating Factors

Attackers will need trick a privileged user to click a link in order to exploit the reflected XSS vulnerabilities.

#### Recommendation

While an official patch has not yet been released by Schneider Electric, Cisco recommends that the following mitigation guide from the Schneider Electric Security Notification be followed:

[https://download.schneider-electric.com/files?p\\_Doc\\_Ref=SEVD-2021-313-03#page=7&zoom=100,93,414](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-313-03#page=7&zoom=100,93,414)

#### 4.20. Insecure Protocol: Network Time Protocol (NTP) Mode 6 Scanner

Severity Rating	MEDIUM	CVSS Score	5.3
CWE Category	CWE-0: Insecure Configuration		
Affected Components	[REDACTED]		

##### Specific Detail

The Team discovered that the remote NTP server responds to mode 6 queries.

##### General Background

The Network Time Protocol (NTP) is used to synchronize device clock times within a network and is intended to synchronize devices within a few milliseconds. This is done through the use of NTP servers, of which there are thousands around the world. An NTP client will issue a time-request exchange with the NTP server, which will then help the client calculate link delay, local offsets, and adjust the local clock to match the server's.

NTP can operate in different modes, which defines the communications between NTP devices. These communications can include NTP client (Mode 3), NTP Server (Mode 4) and NTP control messages (Mode 6). Mode 6 messages are the communication messages for configuration information.

A vulnerability exists in the processing of MODE\_CONTROL (Mode 6) NTP control messages which have a certain amplification vector. An attacker could exploit this vulnerability by sending Mode 6 control requests to NTP servers and clients and observing responses amplified up to 40 times in size.

##### Impact

Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted Mode 6 query, to cause a reflective Denial of Service condition.

##### Recommendation

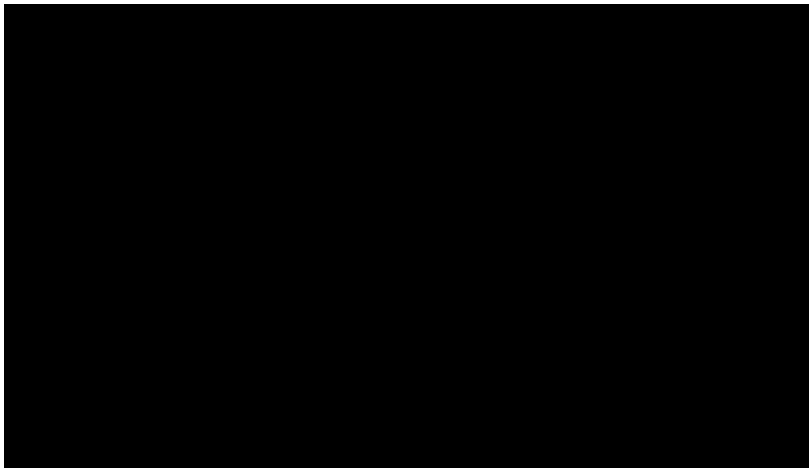
Cisco recommends disabling the service if it is not needed. Otherwise, at a minimum, restrict NTP mode 6 queries.

#### 4.21. Network Camera Detection

Severity Rating	MEDIUM	CVSS Score	5.3
CWE Category	CWE-200: Information Exposure		
Affected Components	[REDACTED]		

#### Specific Detail

The Team discovered remote web servers that were network cameras. Specifically, these cameras had different views of the data center.



*Figure 15 – An Image Showing View Of One Of The Network Cameras Into Data Center Looking At One Of The Data Center Engineers*

#### Impact

An attacker could have a live view of the data center to either target data center employees or keep track of employee movements.

#### Mitigating Factors

The default password to manage the IP camera was not in use, so an attacker would not have been able to control the camera to move the camera or change its parameters.

## Recommendation

Cisco recommends that the live view of the camera be password-protected or disabled by following the instructions from Pelco at:

- <https://support.pelco.com/s/article/Sarix-Changing-the-default-webpage-Disable-Live-View-1538586553946>

#### 4.22. SSL/TLS Service Uses Expired Certificates

Severity Rating	MEDIUM	CVSS Score	5.3
CWE Category	CWE-298: Improper Validation of Certificate - Expiration		
Affected Components	Please see appendix for a full list of all 30 affected components - <a href="#">Full List</a>		

#### Specific Detail

The Team determined that the encrypted service presented a certificate that had already expired, at the time of testing.

#### Impact

An expired SSL/TLS Certificate will generate a warning within the browser during the SSL handshake. This is due to the Certificate Authority policy of issuing certificates on a time-limited basis, to ensure the legitimacy of their services and protect users from compromise by potentially hostile websites. There is no practical security risk associated with this issue as the encryption cipher is still exchanged in exactly the same way as with an unexpired certificate; however, users will likely become used to dismissing security warnings and therefore will become more vulnerable to active “Man-In-The-Middle” attacks, where an attacker presents a fake certificate.

#### Recommendation

Cisco recommends renewing expired SSL Certificates as soon as possible if SSL/TLS continues to be required.

#### 4.23. Insecure Software Version: NTP

Severity Rating	MEDIUM	CVSS Score	5.2
CWE Category	CWE-0: Missing Security Patches		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified that the version of Network Time Protocol Daemon (NTPD) was out-of-date and potentially vulnerable. The ntpd version running on the remote host contains a denial-of-service vulnerability.

#### Impact

Based on behaviours observed in the running NTP server, an attacker could potentially be able to cause a denial-of-service condition or take control of the server as the user running the NTPD service. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial-of-service.

#### Recommendation

Cisco recommends upgrading the NTP server software to the most recent version.

#### 4.24. SNMP Server Weak Community String Configured

Severity Rating	MEDIUM	CVSS Score	5.1
CWE Category	CWE-0: Insecure Configuration		
Affected Components	Please see appendix for a full list of all 30 affected components - <a href="#">Full List</a>		

#### Specific Detail

The Team identified the following weak community string details during testing: public.

#### General Background

Simple Network Management Protocol (SNMP) is a protocol used to collect and modify configuration information for network devices. It uses a community string as an authentication method. The two default strings are private, which will usually allow more sensitive information to be collected and configurations to be changed, and public.

#### Impact

An attacker could query the SNMP service to identify security weaknesses in the system configuration; SNMP servers often disclose information regarding patch level, network configuration and also usernames of accounts that might be present. Such information is often useful to an attacker in preparing an attack. An attacker with knowledge of the read-write SNMP community string could alter device configurations and possibly gain unauthorized access to the device or other devices on the network.

#### Recommendation

Cisco recommends that the SNMP service is reconfigured so that it no longer responds to this community string. Ideally, this would be achieved by disabling community string-based authentication entirely, but if this is not possible, a strong password should be used as the community string. This should be at least 9 characters in length, be composed of the character sets a-z, A-Z, 0-9 and symbols, and should not be based on a dictionary word. In addition, it should not be shared across multiple devices.

#### 4.25. Full Firewall Bypass Via IP Over DNS

Severity Rating	MEDIUM	CVSS Score	4.9
CWE Category	CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak')		
Affected Components	[REDACTED]		

#### Specific Detail

The Team observed that network access controls prevented egress of traffic from the internal environment as accessed by VPN, out to the Internet. However, DNS traffic was not restricted, opening a path for data exchange with hosts outside the internal network environment.

Using the Iodine tool, the Team was able to establish layer 3 IP connectivity to an external endpoint using DNS as the transport. The following images illustrate: connection setup; failed attempt to ping an external host using the default gateway; addition of a route via the Iodine server; and successful ping of an external host via an Iodine link.

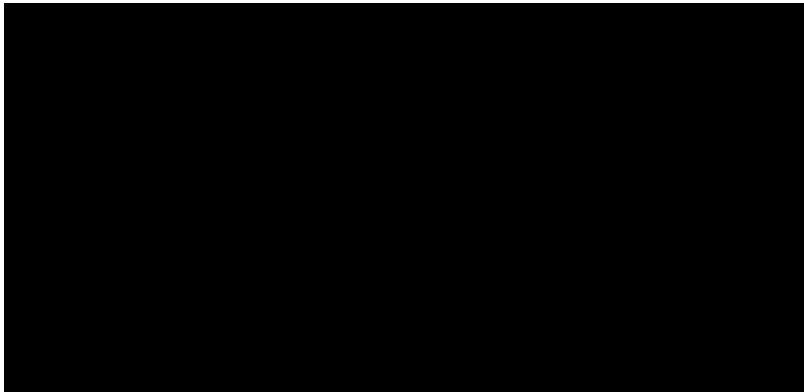
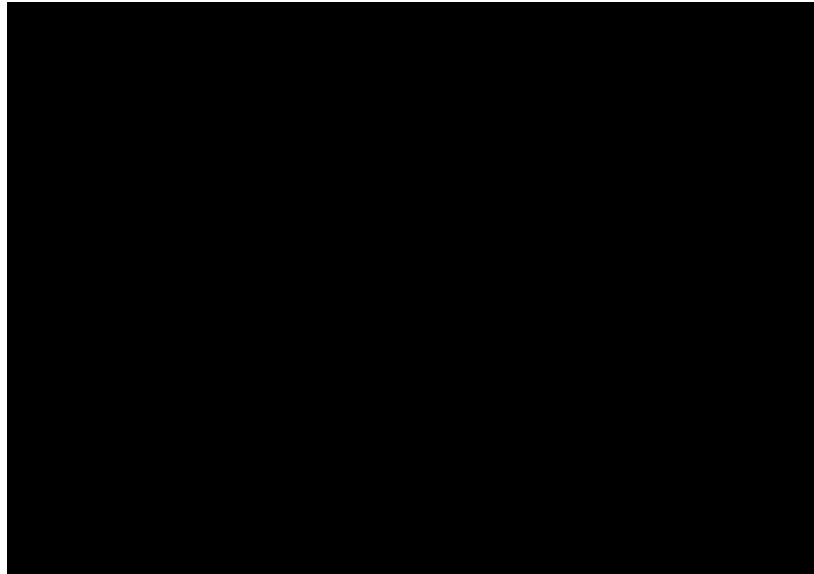


Figure 16 – An Image Showing Use Of Iodine To Establish Layer 3 IP Connectivity Externally





*Figure 17 – An Image Showing Failed Ping Attempt Via Default Gateway, Followed By Successful Ping Via Iodone Link*

#### General Background

Covert channels are an ongoing challenge in secure computing environments, as they rely on unexpected uses of normal behaviours to transmit and/or receive data. Failure to anticipate and block common covert channels may result in unwanted access.

#### Impact

While this example demonstrates fully developed layer 3 IP connectivity, DNS queries can easily facilitate transfer of a variety of information to an external listener. An attacker might use this capability to exfiltrate sensitive data or to remotely control internal systems from the Internet, following a breach.

#### Recommendation

Cisco recommends screening DNS queries for abusive traffic and blocking questionable or unconventionally formed requests. Services such as Cisco Umbrella can identify and prevent unexpected use of DNS.

#### 4.26. NTP 'Monlist' Command Enabled

Severity Rating	MEDIUM	CVSS Score	4.8
CWE Category	CWE-0: Insecure Configuration		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified that the NTP service had the monlist command enabled, allowing the retrieval of a list of recent hosts to connect to the service.

#### Impact

With this command enabled, an attacker could carry out effective network reconnaissance and, along with a spoofed source IP address, carry out an NTP-reflection distributed denial-of-service attack.

#### Recommendation

Cisco recommends either upgrading to NTP 4.2.7-p26 or later or adding "disable monitor" to the ntp.conf file and restarting the service. If, however, these options are not available, then the vendor should be contacted for a patch.

#### 4.27. SMB Server Does Not Support SMB Packet Signing

Severity Rating	MEDIUM	CVSS Score	4.6
CWE Category	CWE-0: Insecure Configuration		
Affected Components	[REDACTED]		

#### Specific Detail

The Team determined that the "Microsoft network server: Digitally sign communications (if client agrees)" policy was set to "Disabled", causing SMB traffic to be unsigned and subject to tampering.

#### Impact

An attacker may be able to execute a successful Man-in-The-Middle attack against communications and inject traffic into the established data stream, which could have consequences including data loss, data corruption, privilege escalation and ultimately system compromise. By failing to require incoming SMB connections to be signed, all such connections will be vulnerable to such attacks if the attacker is able to alter network traffic between the client and server. Furthermore, SMB clients configured to mandate signing (in accordance with good security practice) will not be able to communicate with the host.

#### Recommendation

Cisco recommends enabling this policy.

Using the relevant local security policy editor, domain controller security editor or group policy editor (GPO), the recommended policy setting can be updated on the system by navigating to:

Local Policies / Security Options / Microsoft network server: Digitally sign communications (if client agrees)

Note: Implementing this recommendation may still leave incoming connections vulnerable to a downgrade attack, where a client and server both support signing but an attacker modifies the negotiation to avoid signing being used. To protect against this, also enable 'Microsoft network server: Digitally sign communications (always)'.

#### 4.28. SNMP 'GETBULK' Reflection Distributed Denial-Of-Service

Severity Rating	MEDIUM	CVSS Score	4.6
CWE Category	CWE-0: Insecure Configuration		
Affected Components	<div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div>		

#### Specific Detail

The Team identified that the SNMP daemon was vulnerable to a reflected distributed denial-of-service attack due to the response to a 'GETBULK' request being larger than the normal value for max repetitions.

Component	Details
<div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div>	<p>Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack:</p> <p>Request size (bytes) : 42</p> <p>Response size (bytes) : 1349</p>
<div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div>	<p>Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack:</p> <p>Request size (bytes) : 42</p> <p>Response size (bytes) : 1349</p>
<div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div>	<p>Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack:</p> <p>Request size (bytes) : 42</p> <p>Response size (bytes) : 1349</p>
<div style="background-color: black; width: 100px; height: 15px; display: inline-block;"></div>	<p>Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack:</p> <p>Request size (bytes) : 42</p>

	Response size (bytes) : 1349
████████████████████	Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack: Request size (bytes) : 42 Response size (bytes) : 1349
████████████████████	Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack: Request size (bytes) : 42 Response size (bytes) : 1350
████████████████████	Nessus was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack: Request size (bytes) : 42 Response size (bytes) : 1349

### Impact

With a large amount of data being included in the response to a 'GETBULK' request, a remote attacker could use the SNMP server to conduct a reflected distributed denial-of-service attack on another arbitrary host.

### Recommendation

Cisco recommends disabling the SNMP service if it is not required. Otherwise, access to this service should be restricted and monitored and the default 'public' community string changed.

#### 4.29. Insecure Protocol: Telnet

Severity Rating	MEDIUM	CVSS Score	4.2
CWE Category	CWE-319: Transmission of Sensitive Information In Plain Text		
Affected Components	[REDACTED]		

#### Specific Detail

The Team identified the presence of the plain text Telnet service.

The following screenshot illustrates the recovery of username (root) and password (REDACTED) from captured network traffic.

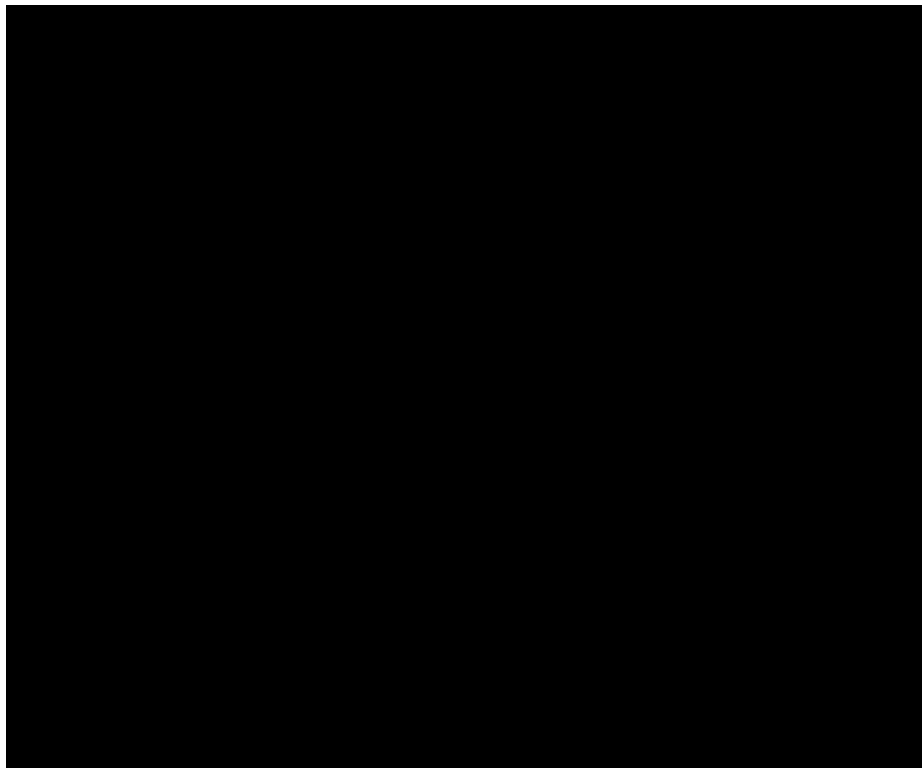


Figure 18 – Image Showing Captured Network Traffic Decoded to Recover Username and Password

### Impact

An attacker able to access the network between the client and server could hijack authenticated sessions, including an administrator's. Usernames and passwords might also be retrieved via eavesdropping and used in subsequent attacks.

### Recommendation

Cisco recommends that, where possible, the Telnet service is replaced with the more secure SSH protocol version 2. When used correctly, SSH is not vulnerable to password eavesdropping attacks or session hijacking.

# Appendices

---

## Appendix A: Internal Infrastructure Assessment

### APPENDIX A.1: DEFAULT PASSWORDS PRESENT ON SERVER

Component
[REDACTED]

### APPENDIX A.2: IPMI PROTOCOL VULNERABLE TO PASSWORD HASH RETRIEVAL

Component
[REDACTED]

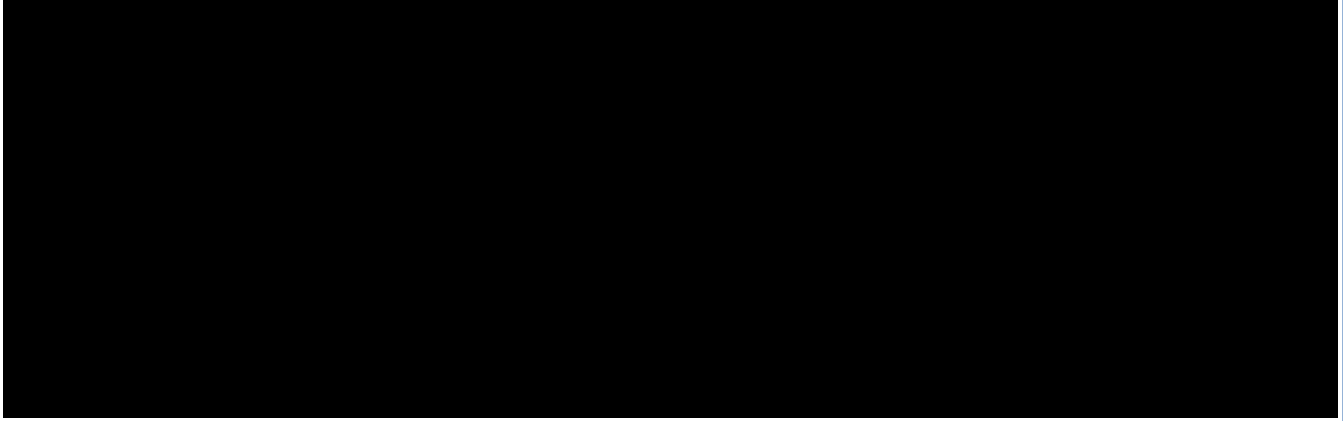
### APPENDIX A.3: SSL/TLS SERVICE USES EXPIRED CERTIFICATES

Component
[REDACTED]



#### APPENDIX A.4: SNMP SERVER WEAK COMMUNITY STRING CONFIGURED

Component



## Appendix B: Definition of Terms

Each finding identified during the assessment is allocated a Severity Level and CVSS 3.0 score; the Severity Level being directly derived from the CVSS 3.0 score as per the standard, as well as being described under the Specific Details, Security Impact and Recommendations headings, with an additional Steps to Reproduce header, where applicable. The ratings are based on the individual objective finding and not the subjective risk the issue may pose.

### CVSS

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS consists of 3 groups: Base, Temporal and Environmental.

Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics. These metric groups are described as follows:

- Base: represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and across user environments.
- Temporal: represents the characteristics of a vulnerability that may change over time but not across user environments.
- Environmental: represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

Cisco uses the CVSS 3.0 scoring mechanism and directly maps those to severity ratings for each finding, as defined in the CVSS 3.0 standard shown below:

Severity Rating	CVSS Score
Critical	9.0 – 10.00
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
None	0.0

## CWE

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

Cisco applies a relevant CWE against each finding in order to allow for finding grouping, which is then used to generate the remediation action plan in the recommendations section of the report.

## Appendix C: Why Cisco Assessment and Penetration Team?

Cisco's Assessment and Penetration Team is comprised of a combination of in-house consultants, as well as the acquisition of the widely recognized and respected Information Security service providers Neohapsis and Portcullis, which constitutes a long pedigree of technical excellence and industry-defining capabilities.

Cisco's Assessment and Penetration Team delivers a vast array of Security Consultancy and Technical Assurance engagements whilst leveraging Cisco's real time intelligence sources, providing a realistic view of the threats to an organization. With a deep understanding of the Tactics, Techniques and Procedures (TTPs) used by modern technical adversaries, Cisco's Assessment and Penetration Team can assess our customers' systems (both technical and procedural) to identify any vulnerabilities or weaknesses, which could be utilized by an attacker. In situations where an attack has been successful, Cisco have the capability to assist our clients in understanding the chain of events that lead up to the breach. This enables our clients to improve systems and policies they have in place to ensure that similar attacks are not successful in the future.

The vast experience of Cisco's Assessment and Penetration Team, along with our blended service offerings, enable us to deliver comprehensive security solutions such as long-term strategic roadmaps down to tactical and technical remediation steps for our customers', as Trusted Advisors and a dependable security partner throughout the development and growth of a business.

This strong pedigree is further augmented by our array of industry and global accreditations, including certified CHECK Team Leaders/Members and CREST STAR (CCSAM and CCSAS), as well as PCI/ISO Qualified Security Assessors, FIRST membership, NCSC's CiSP and the full weight of Cisco's extremely talented technical and engineering teams.

With a client base encompassing Central and Local Government, Banks, Manufacturing, Charities, Global Service Providers, Utilities, Insurance, Retail, Healthcare, Energy, Education, Fast Moving Consumer Goods, Technology, Financial Services, Media and many international Blue Chip clients operating across the globe, Cisco Assessment and Penetration Team's breadth of expertise and experience is second to none.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam.  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



# Cisco Security Services



SampleCo

Wireless Penetration Test

March 20, 2023

Technical Report

1.0

COMMERCIAL-IN-CONFIDENCE



## About This Document

Document Information	
<b>Author</b>	Mark Wnghraifft
<b>Change Authority</b>	Cisco Systems Customer Experience

Document History			
Version	Date	Status	Comments
0.5	March 18, 2023	Draft	1st Draft - Cisco
1.0	March 20, 2023	Final	Revised and Final

Document Review		
Reviewer	Version	Date
Vince Sampla	0.5	March 19, 2023

This document contains and constitutes the proprietary and confidential information of Cisco (“Cisco”). It is provided to Cisco Example Account (“Company”) subject to and in accordance with the terms of any agreement between Cisco and the Company regarding treatment of confidential information and/or licensing of proprietary information. This document also contains information that is highly sensitive confidential information of the Company and should be treated by representatives of the Company accordingly. This document may not be distributed by the recipient without the express permission of Cisco and the Company.

The contents of this document do not constitute legal advice. Cisco’s offer of services or deliverables that relate to compliance, litigation, or other legal interests is not intended as legal counsel and should not be taken as such.



# Table of Contents

Table of Contents .....	5
1. Executive Summary .....	7
1.1 Introduction .....	7
1.2 Conclusions.....	7
1.3 Recommendations.....	8
RECOMMENDED ACTION PLAN .....	8
2. Project Summary .....	9
2.1 Project Scope.....	9
2.2 Project Teams .....	9
3. Technical Analysis .....	10
3.1 Technical Summary .....	10
3.2 Summary of Findings.....	11
STRENGTHS.....	11
WEAKNESSES .....	11
INDEX OF FINDINGS .....	13
4. Wireless Penetration Test.....	14
Appendices .....	32
Appendix A: WPA2-Enterprise Security Overview.....	32
SUMMARY OF WPA2-ENTERPRISE PROTOCOLS .....	32
EVIL TWIN ATTACKS TARGET USER CREDENTIALS .....	32
INCREASING DETECTION RECOMMENDATIONS .....	33
USE EAP TYPES WITH MUTUAL AUTHENTICATION TO LIMIT ATTACKS .....	33
Appendix B: Wireless Penetration Test Methodology .....	34
WIRELESS NETWORK ENUMERATION .....	34

DIRECT EVALUATION OF WIRELESS NETWORKS .....	34
ROGUE ACCESS POINT ATTACKS AGAINST WIRELESS CLIENTS .....	34
Appendix C: CVSS Vector Strings .....	35
WIRELESS PENETRATION TEST .....	35
Appendix D: Definition of Terms .....	37
CVSS .....	37
CWE .....	38

# 1. Executive Summary

---

## 1.1 Introduction

SampleCo engaged Cisco to conduct a wireless penetration test against the networks used at their headquarters campus. A wireless penetration test is a type of "ethical hacking" or "intrusion testing" approach for detecting vulnerabilities in wireless infrastructure configuration. The assessment had the following goals:

- Evaluate whether devices and networks are configured in line with current guidelines
- Attempt to use any weakness to breach or evade network protections and access the internal corporate network

Testing took place between the March 12 and March 16, 2023.

Cisco assessed the networks at the facilities specified by SampleCo:

- Head Office at XXXXX,XXXX

The assessment took place during normal working hours to effectively assess the behavior of the network and observe representative traffic between its nodes.

## 1.2 Conclusions

Cisco found multiple high risk issues within SampleCo's network infrastructure:

- Cisco captured user credentials using rogue access point attacks
- Cisco found default administrator credentials in use
- Cisco successfully reconstructed the weak pre-shared key for the *BYOD* network
- Cisco found unencrypted wireless networks in use

These flaws allowed Cisco to gain direct access to the internal corporate network and to authenticated SampleCo services.

In addition, Cisco found a wide variety of configuration issues that facilitated these high level issues. SampleCo should take immediate action to remediate the findings of this report and reduce the attack surface of its wireless networks.

## 1.3 Recommendations

### RECOMMENDED ACTION PLAN

#### Evaluate Monitoring and Data Protection on Guest Networks

SampleCo has a stated desire for easy access to its *Guest* network and has implemented a simple terms of service acceptance to gate access. To reduce the risk of misuse, Cisco recommends implementing additional monitoring technologies that ensure that any breaches of the terms of service is detected and logged. Additionally, Cisco recommends ensuring SampleCo restricts usage to commonly used ports, implementing bandwidth restrictions, and enforcing timeouts on connected clients.

#### Improve Key and Privileged Account Management

SampleCo's networks used weak pre-shared keys and devices were still configured with default credentials. Pre-shared key networks for managed devices should use strong keys that are rotated quarterly, preferably managed through a mobile device management system. Network devices should have their default settings changed during deployment and SampleCo should consider an enterprise-wide privileged account management solution.

#### Use EAP-TLS Whenever Possible

Cisco was able to compromise credentials using a Rogue AP by exploiting lack of validation in the PEAP authentication protocol. LADWP should use EAP-TLS whenever possible for its authenticated networks. Appendix A contains a fuller exploration of WPA2 Enterprise security.

#### Configure systems in line with industry good security practice

SampleCo's wireless devices exhibit a variety of poor configuration choices that could enable an attacker to obtain a foothold within the network or environment. Poor configuration includes the retaining of vendor-supplied default settings and/or passwords, which can often be easily guessed, and services being enabled unnecessarily.

All systems within the IT environment should be reviewed and their configurations brought into line with industry good security practice guidelines. In addition, strict change control should be applied with regards to all production systems.

## 2. Project Summary

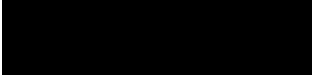
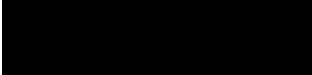

Members of the Cisco Advisory team have served as trusted business advisors, cyber security leaders, and technical experts in a wide range of roles. Together we use our vast experience in cyber security, risk management, and technical innovation to help our clients across every industry advance their business objectives.

### 2.1 Project Scope

Cisco assessed the networks at the facilities specified by SampleCo:

- Head Office at XXXXX,XXXX

The following wireless ESSID identifiers were in scope:

- 
- 
- 

### 2.2 Project Teams

Cisco Project Team		
Team Member	Project Role	Contact Information
Mark Wnghraifft	Team Lead	marwnghr@cisco.com
Barry Ekzemplo	Project Manager	baekzemp@cisco.com

SampleCo Project Team		
Team Member	Project Role	Contact Information
Bob Tusaale	Executive Accountant	bob@sampleco.com

## 3. Technical Analysis

---

### 3.1 Technical Summary

#### Initial Network Scanning

Cisco began the assessment by conducting reconnaissance scans of the 2.4GHz and 5GHz signal bands in Building 1. Scanning revealed a few trends:

- The vast majority of detected SSIDs come from Cisco infrastructure
- A number of open guest networks were served by Virgin Mobile SuperHub devices
- There were no detectable access points from outside Building 1

#### Collecting WPA2 Handshakes and PMKIDs

All security in a WPA2 using pre-shared keys (WPA2-PSK) use four packets to handle key exchange. This four-way handshake is a protocol level weak point in all WPA2-PSK networks and puts them at risk to offline cracking attacks. A large number of devices connect to the WPA2-PSK [REDACTED] network and Cisco was able to passively collect handshakes from without actively deauthing any devices.

Cisco also tested direct PMKID extraction and found that some infrastructure is vulnerable to this attack. The PMKID was developed for fast roaming and can and can be attacked through offline cracking to reverse a network's pre-shared key.

#### Reversing the Weak PSK on BYOD

Once Cisco collected the four-way handshake and PMKID, it used a GPU based cracking rig to reverse the pre-shared key for [REDACTED]. This pre-shared key is a dictionary word and number [REDACTED].

#### Rogue AP Testing

Using the eaphammer tool, Cisco created a rogue AP outside a conference room on the second floor. Cisco was able to entice several devices to connect to the Rogue AP. eaphammer attempts to negotiate the weakest authentication mechanism. In this case The Rogue AP was able to negotiate clients down to EAP-GTC which uses plain-text credentials. Cisco collected one username and password during during 10 minutes of testing time.

## Guest Network Testing

Cisco conducted testing of the [REDACTED] network. Cisco tested the segmentation and security settings of these networks both before and after authorization. [REDACTED] uses a captive portal setup. During testing, Cisco:

- Connected to administrative control pages from the guest network and log in with default credentials
- Bypassed the captive portal by spoofing a previously associated client
- Used DNS to connect to outside DNS servers and extract gratuitous information from responses
- Connected to other devices associated to the wireless network

## 3.2 Summary of Findings

### STRENGTHS

Access Points were not physically accessible from outside areas restricted to staff.

### WEAKNESSES

#### Use of Default Credentials

##### DESCRIPTION

The use of default credentials presents a significant security risk, as they are often publicly known.

##### SOLUTION

Ensure, prior to deployment, that all devices have default credentials changed to suitably secure values.

#### Insufficient Network Segregation

##### DESCRIPTION

The unsegregated nature of the network environment could allow unchecked traversal across the infrastructure once a single point had been compromised, and this must be addressed. An example of good practice in this regard is the separation of a live production environment from the development/test environment, where security practice is often overlooked; otherwise a compromise of the development environment would very possibly lead to a trivial compromise of the production/financial environment.

##### SOLUTION

By implementing good network segregation, the possibility of an attacker being able to compromise more than a single zone is significantly reduced. It is recommended that the network infrastructure is segregated into security zones (by utilising VLAN and internal firewalls) to achieve greater strength-in-depth within the infrastructure.

## Insufficient Access Controls

### DESCRIPTION

Access controls are not implemented properly, allowing users to access functionality outside of their intended remits.

### SOLUTION

Ensure Access Control Lists are correctly implemented to ensure that services intended to be accessed only at certain points are properly segregated.

## Weak Cryptographic Protection

### DESCRIPTION

The supported cryptographic methods allowed a number of weak algorithms to be used, compromising the confidentiality and integrity of sessions and user data. Certificates are central to the prevention of "Man-In-The-Middle" attacks and must be monitored to ensure that they are valid and in-date.

### SOLUTION

Ensure that only strong ciphers, free of cryptographic flaws, are supported by the server and regularly check to ensure that all server certificates are valid in every respect to minimise the possibility of an attacker tricking users into connecting to a rogue server.

## Insecure Configuration

### DESCRIPTION

Insecure configuration can lead to sensitive information being disclosed, or services being exposed to attack.

### SOLUTION

Modify the current configuration files to ensure they adhere to good practice principles, and conduct regular configuration reviews to ensure that current variables are up-to-date with latest industry good security practice guidelines.



## INDEX OF FINDINGS

Finding Title	Severity Rating	CVSS Score
1. Weak Pre-Shared Keys In Use	HIGH	8.2
2. Default Device Credentials In Use	HIGH	7.6
3. Open Wireless Networks In Use	HIGH	7.3
4. PEAP Vulnerable To "Rogue AP" Attacks	HIGH	7.3
5. Client Configuration Does Not Define RADIUS Certificate CommonName	HIGH	7.1
6. Admin Interfaces Presented To Guest Wireless Network	MEDIUM	6.5
7. MAC Spoofing Allows Guest Network Access	MEDIUM	6.3
8. Access Points Using WiFi Protected Setup (WPS)	MEDIUM	6.2
9. Access Points Allow PMKID Extraction	MEDIUM	5.8
10. WPA2-PSK Allows Handshake Collection	MEDIUM	5.4
11. Gratuitous Information Disclosed Within DNS Server Responses	MEDIUM	5.3
12. Wireless Client Isolation Not Enabled	MEDIUM	5.2
13. Internet-Based DNS Queries Allowed Prior To Authorization	MEDIUM	4.1

## 4. Wireless Penetration Test

### 4.1. Weak Pre-Shared Keys In Use

Severity Rating	<b>HIGH</b>	CVSS Score	<b>8.2</b>
CWE Category	CWE-521: Weak Password Requirements		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco found multiple weak keys in use:

- Cisco cracked the PSK for [REDACTED] after collecting the PMK (issue [4.10](#)). Offline password cracking successfully recovered the PSK [REDACTED]

#### General Background

Allowing weak or publicly known pre-shared keys or passwords makes them vulnerable to brute-force. For wireless PSKs weak passwords can be reversed offline once a four way handshake or PMKID has been successfully captured.

#### Impact

The [REDACTED] network has direct access to some internal networks. An attacker could use their foothold in [REDACTED] to compromise one of these systems then move laterally to other networks in the environment.

#### Mitigating Factors

- [REDACTED] does not have full internal network access

## Recommendation

Cisco recommends:

- WPA2 PSKs can be up to 63 characters long, implement the longest key that client devices can support
- Use Mobile Device Management software to regularly rotate the PSK on managed devices
- PSKs should consist of a mix of upper and lower case characters, at least one number and at least one non-alphanumeric character
- Reject any PSK that contains a dictionary word

If these recommendations cannot be implemented, restrict the [REDACTED] network from any internal networks.

## 4.2. Default Device Credentials In Use

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.6</b>
CWE Category	CWE-798: Use of Hard-coded Credentials		
Affected Components	[REDACTED]		

### Specific Detail

Cisco found the admin logins for Virgin Media SuperHubs installed at all physical locations had the default username and password:

Component	Details
[REDACTED]	login: [REDACTED] password: [REDACTED]

### General Background

Default credentials are not meant to be used for the operational life of the device. In some cases the default credentials maybe available in documentation or are written on the device. Many public and private repositories collect default credentials and these can help attackers quickly find the default credentials.

### Impact

Cisco was able to log into the access point from the guest network. An attacker gaining access to the SuperHub either physically or via the wireless network could reconfigure the device and deny access to legitimate users or attempt to subvert network traffic to another device under their control.

## Recommendation

Cisco recommends that domain passwords are audited on a regular basis for the presence of weak passwords, and that an appropriate password policy consisting of a defined set of rules is put in place (if not already present). Where password policy changes have been retroactively applied to a system, all account passwords should be forcibly changed to comply with the new policy.

NIST Special Publication 800-63B recommend that organizations:

- Set passwords rules that allow a minimum length of eight characters and no maximum
- Not allow passwords that incorporate the company name, application name, common words, or the user's name

Note: Adding numbers as a prefix or suffix to dictionary words is not effective protection from cracking attacks. For service accounts, Cisco recommends the following over the standard password policy recommendations:

- Service account passwords should not be shared between accounts
- Service accounts should at least be 15 characters and as long as can be supported by the underlying application
- Service account passwords should be stored in a secrets management system designed to facilitate secure storage and regular rotation

### 4.3. Open Wireless Networks In Use

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.3</b>
CWE Category	CWE-311: Sensitive Data Not Encrypted		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco discovered the following Open (OPN) wireless networks:

- [REDACTED]

#### General Background

The Open network is the simplest authentication type for an 802.11 wireless network. These networks do not encrypt data traffic from devices to the access point and by default will allow any device to associate to them.

#### Impact

With no encryption in place and data being sent/received in plain text, a malicious user could eavesdrop a user's traffic and potentially capture credentials for other online services.

#### Mitigating Factors

[REDACTED] uses a captive portal to limit access to the network and generally limits access to internal network resources.

#### Recommendation

Cisco recommends that secure encryption such as WPA2 'Enterprise' be implemented and enabled on the access points. A good solution which follows secure industry practices is to configure a guest to the Ambassador mechanism, where a guest must ask a member of staff who can generate them a temporary RADIUS account and credentials, which will expire after a set amount of time.

#### 4.4. PEAP Vulnerable To "Rogue AP" Attacks

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.3</b>
CWE Category	CWE-345: Insufficient Verification of Data Authenticity		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco found that [REDACTED] uses WPA Enterprise with Protected Extensible Authentication Protocol (PEAP). Cisco set up a fake access point using the eaphammer toolkit near an employee meeting room and waited for devices to connect. Cisco's fake access point requested that associating device downgrade to the EAP-GTC protocol so that it would submit plain-text credentials instead of hashed or mutually authenticated credentials.

#### General Background

Rogue AP attacks focus on attacking the wireless clients of a network and rely on the fact that the 802.11 standards do not provide a mechanism for access points (APs) to authenticate themselves. They may be conducted on-site by attempting to coerce clients to connect to them or off-site at a location commonly trafficked by members of a target organization.

#### Impact

Cisco's captured the plaintext credentials of one mobile device attempting to authenticate to [REDACTED].

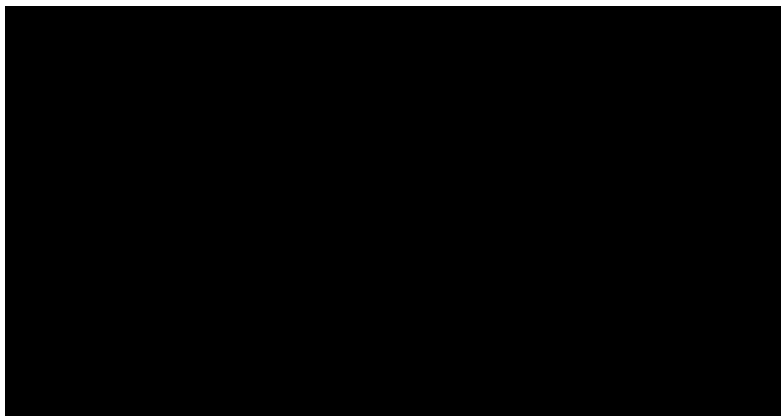


Figure 1 – Successful eaphammer capture of account credentials

Cisco used these credentials to gain full access to the corporate network and authenticate directly to the Windows Domain using the stolen credentials.

### Mitigating Factors

The user was required to click a certificate warning before the fake AP received user credentials.

### Recommendation

Cisco recommends that that WPA-Enterprise networks consistently:

- Avoid internal EAP types that allow hash or credential collection (GTC, MD5, FAST, MSCHAPV2)
- Use certificate based EAP methods that authenticate devices instead of using credentials
- Educate users on the risks of connecting to rogue networks

Additionally, rogue AP detection equipment should be introduced to the premises ('wireless' IPS/IDS) to detect new/malicious APs.



#### 4.5. Client Configuration Does Not Define RADIUS Certificate CommonName

Severity Rating	<b>HIGH</b>	CVSS Score	<b>7.1</b>
CWE Category	CWE-599: Trust of OpenSSL Certificate Without Validation		
Affected Components	[REDACTED]		

#### Specific Detail

While directly examining a Window 7 test device provided to Cisco, they observed that the client configuration did not validate the RADIUS certificate appropriately.

#### Impact

If the CommonName for the trusted server is not specified, clients can connect to any trusted or untrusted server (based on the client configuration) without validating the CommonName.

#### Recommendation

Cisco recommends that the CommonName for the trusted server is set in the client's configuration.

#### Steps to Replicate

MS Windows 7 client:

- 1) Open the Control Panel.
- 2) Click on "View network status and tasks".
- 3) Click on "Manage network connections".
- 4) Right click on a "PEAP" connection and select "Properties".
- 5) In the "Security" tab, click on "Settings".
- 6) The text field "Connect to these servers:" should be validated with the RADIUS certificate's CommonName.

#### 4.6. Admin Interfaces Presented To Guest Wireless Network

Severity Rating	MEDIUM	CVSS Score	6.5
CWE Category	CWE-0: Insecure Configuration		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco found that wireless network admin interfaces were accessible to clients on the [REDACTED] network including:

- Cisco ISE devices
- Virgin Media SuperHubs

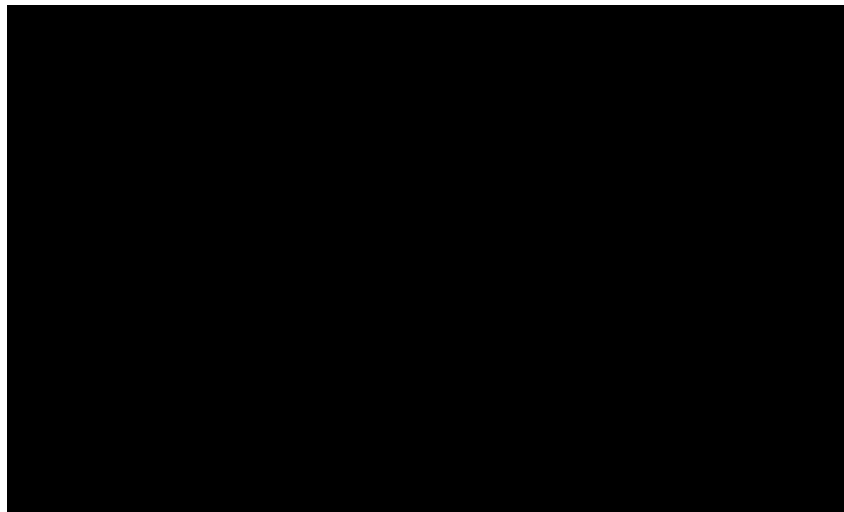


Figure 2 - An Image Showing The Availability Of The Cisco ISE Admin Interface

#### General Background

Whether a device can be managed over the wireless networks it serves is typically a configurable option on the device.

## Impact

Cisco used the default credentials on the Virgin Media Superhubs to gain admin access through their exposed login portals (Finding 4.2) from the [REDACTED] network.

In general, presenting the admin interfaces to the [REDACTED] wireless network could allow either an authorized or unauthorized malicious user to directly attack the Cisco ISE. By exploiting a flaw within the ISE, or brute-forcing access credentials, the attacker might then be able to gain access to the ISE and leverage this access to conduct further attacks against the Client's networks or systems.

## Recommendation

Cisco recommends:

- Restricting administrative interfaces so that they can only be accessed from the wired network
- Segmenting the guest network away from other internal networks and only exposing [REDACTED] web page
- Limiting the services used on the [REDACTED] network

### 4.7. MAC Spoofing Allows Guest Network Access

Severity Rating	MEDIUM	CVSS Score	6.3
CWE Category	CWE-0: Insecure Configuration		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco found that the [REDACTED] network used MAC filtering to determine whether a device had authenticated to the "guestportal" site.

#### General Background

Captive portal guest networks routinely use MAC filtering to decide whether a device is allowed to access resources. MAC addresses are part of all network traffic and can easily be viewed by an attacker.

#### Impact

Cisco gained access to the [REDACTED] network by impersonating the MAC address of an authenticated client.

#### Recommendation

Cisco recommends changing the [REDACTED] wireless network from OPN (Open) to WPA2-PSK while still using the [REDACTED] authorization page.

### 4.8. Access Points Using WiFi Protected Setup (WPS)

Severity Rating	MEDIUM	CVSS Score	6.2
CWE Category	CWE-0: Insecure Configuration		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco found Wi-Fi Protected Setup (WPS) enabled on the [REDACTED] network Virgin Media SuperHub routers installed at all physical locations.

#### General Background

Wi-Fi Protected Setup was developed in 2006 to simplify wireless home network setup. The WPS protocol relies on EAP messages that are triggered by user interaction (e.g. a user presses a button on a router then another button on a WPS network device).

#### Impact

There have been a number of publicly disclosed vulnerabilities in connection with the WPS service that could allow an attacker to obtain the wireless WPA2 Pre-Shared Key passphrase by brute-forcing the WPS PIN code. An attacker could also gain access to the affected network by brute-forcing WPS pin codes.

#### Mitigating Factors

Cisco was unable to successfully exploit WPS on the affected devices.

#### Recommendation

Cisco recommends deactivating WPS for all Access Points.

#### 4.9. Access Points Allow PMKID Extraction

Severity Rating	MEDIUM	CVSS Score	5.8
CWE Category	CWE-696: Incorrect Behaviour Order		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco successfully collected EAPOL frames containing the PMKID from access points providing the [REDACTED] network.

#### General Background

This attack directly attacks the affected access point without capturing the WPA2 four way handshake from a client device. The PMKID is an optional feature of the 802.11 security standard that was intended to provide faster roaming between access points in a single frame instead of a full handshake. The PMKID is an HMAC-SHA1 derived from the true Pairwise Master Key and other elements that can be extracted from the EAPOL frame. In 2018, the hashcat team announced that a pre-shared key could be reversed using only an EAPOL frame with a PMKID for the target network.

#### Impact

Cisco used the extracted PMKID to reverse the weak pre-shared key (PSK) for the *BYOD* network (Finding 4.1).

#### Recommendation

Cisco recommends disabling PMKID Caching (aka Sticky Key Caching).

### 4.10. WPA2-PSK Allows Handshake Collection

Severity Rating	MEDIUM	CVSS Score	5.4
CWE Category	CWE-0: Weak Cryptographic Protection		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco scans showed the [REDACTED] network configured with a WPA2 pre-shared key.

Furthermore, the Team was able to de-authenticate a valid device from the [REDACTED] network and capture the 4-way handshake as it reconnected to the access point. This

#### General Background

WPA2's Extensible Authentication Protocol (EAPOL) uses a sequence of for EAPOL frames to establish encrypted communications between the client device and the access point. If an attacker can capture this "four way handshake" they have enough information to reconstruct the Pairwise Transient Key and pass it to offline cracking tools to recover the network's pre-shared key.

#### Impact

Cisco was able to reverse the pre-shared key using an offline attack, allowing the Team to successfully authenticate to the network due to a weak password being used (see issue [4.1](#)).

#### Recommendation

Cisco recommends:

- WPA2 PSKs can be up to 63 characters long, implement the longest key that client devices can support
- Use Mobile Device Management software to regularly rotate the PSK on managed devices
- PSKs should consist of a mix of upper and lower case characters, at least one number and at least one non-alphanumeric character
- Reject any PSK that contains a dictionary word

If these recommendations cannot be implemented, restrict the [REDACTED] network from any internal networks.

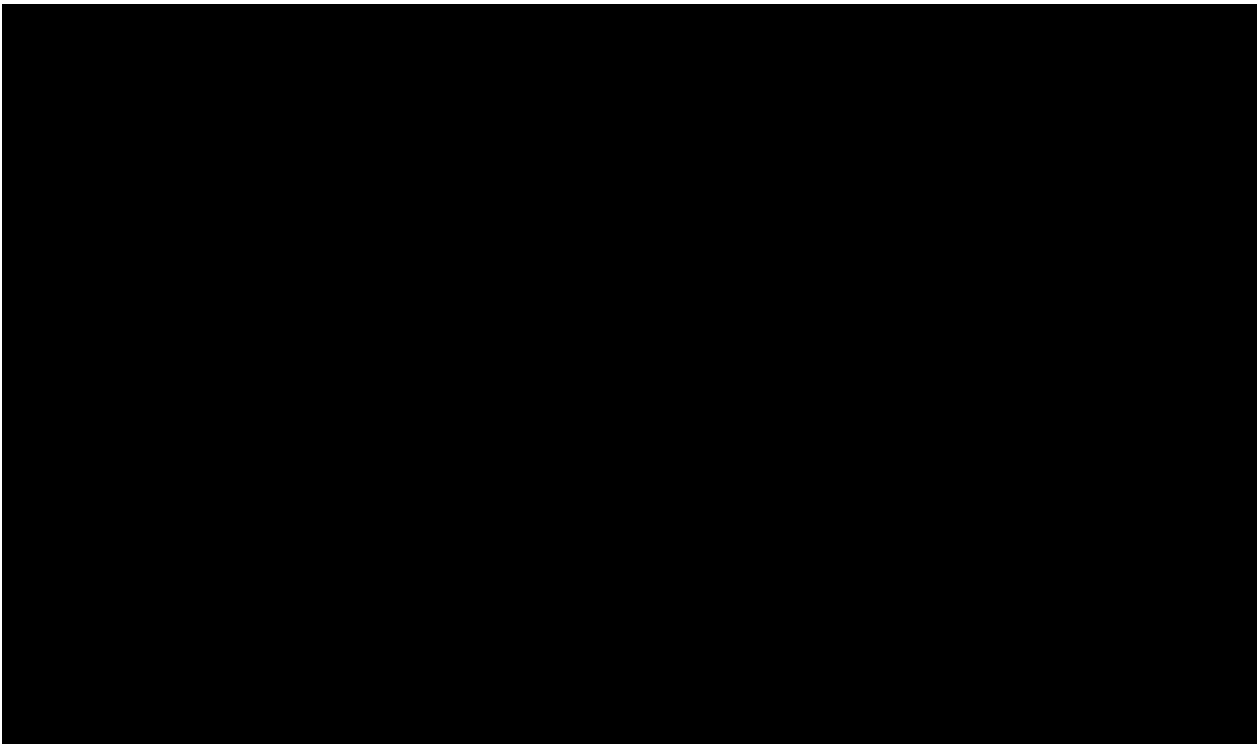
#### 4.11. Gratuitous Information Disclosed Within DNS Server Responses

Severity Rating	MEDIUM	CVSS Score	5.3
CWE Category	CWE-200: Information Exposure		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco observed that it was possible to retrieve version information from the DNS server using specific DNS query requests for *version.bind* in the 'CHAOS' domain.

The following details were retrieved:



Note: The version details are not strictly accurate and could even be forged, as some DNS servers send the information based on a configuration file.



## General Background

The Domain Name System is the naming computer systems and services and provides network protocols for resolving these names into IP address.

## Impact

With the version information leaked, an attacker could quickly establish whether there are any vulnerabilities within the DNS service that can be exploited.

## Recommendation

Cisco recommends that this specific information leakage is prevented (it may be necessary to refer to the vendor documentation on how to disable the relevant settings).

## 4.12. Wireless Client Isolation Not Enabled

Severity Rating	<b>MEDIUM</b>	CVSS Score	<b>5.2</b>
CWE Category	CWE-0: Insufficient Network Segregation		
Affected Components	██████████		

### Specific Detail

Cisco discovered that Wireless Client Isolation was not enabled on the access point and that another client on the █████ network could be identified and attacked.

### General Background

Wireless Client Isolation is a feature of wireless access points that prevents associated clients from directly communicating with each other.

This setting can also be known as Wireless client security separation or peer-to-peer blocking.

### Impact

Wireless Client Isolation prevents devices connected to the wireless access point from being able to connect to each other, which is aimed at preventing an attacker that manages to obtain access to the network from being able to attack other wireless devices.

### Recommendation

Cisco recommends enabling Wireless Client Isolation.

### 4.13. Internet-Based DNS Queries Allowed Prior To Authorization

Severity Rating	MEDIUM	CVSS Score	4.1
CWE Category	CWE-284: Insufficient Access Controls		
Affected Components	[REDACTED]		

#### Specific Detail

Cisco found that clients connecting to the [REDACTED] wireless network could access the Internet on port 53/UDP, prior to authentication through the Captive Portal.

#### General Background

The Domain Name System is the naming computer systems and services and provides network protocols for resolving these names into IP address.

#### Impact

It might be possible for an attacker to connect to the [REDACTED] network and obtain Internet connectivity without authentication by tunneling traffic over port 53/UDP to a Internet-based server, for example, by establishing an OpenVPN connection using that port.

#### Recommendation

Cisco recommends that access to the Internet on any port, either TCP or UDP, is prohibited without prior authentication.

# Appendices

---

## Appendix A: WPA2-Enterprise Security Overview

### SUMMARY OF WPA2-ENTERPRISE PROTOCOLS

With the wide variety of wireless authentication protocol choices available it can be difficult to make reasonable choices about security risk. As of 2010 the Wi-Fi Alliance certified eight different EAP types, with one layer that performs the authentication and another that protects that communication and fall into two categories:

- EAP types that mutually authenticate devices (EAP-TLS)
- EAP types that authenticate a user's credentials (EAP-TTLS/MSCHAPv2, PEAP/EAP-MSCHAPv2, PEAP/EAP-GTC)

EAP types that mutually authenticate devices are the most secure since they can ensure that only authorized devices can connect to a Wireless network. EAP types that authenticate user credentials are often susceptible to Evil Twin attacks, which mimic a target's wireless infrastructure in attempt to induce a client to connect and submit plain-text or hashed credentials.

### EVIL TWIN ATTACKS TARGET USER CREDENTIALS

Evil Twin attacks focus on attacking the wireless clients of a network and rely on the fact that the 802.11 standards do not provide a mechanism for access points (APs) to authenticated themselves. An attacker has several ways to attempt get wireless devices to associate with a malicious access point:

- Abusing 802.11 roaming
  - Entice clients to entice clients to connect by providing better signal strength
  - Coerce clients to connected by blocking access to legitimate access points
- Responding to client probes for a target network when away from campus (Karma and MANA attacks)
- EAP types that authenticate users (EAP-TTLS/MSCHAPv2, PEAP/EAP-MSCHAPv2, PEAP/EAP-GTC)

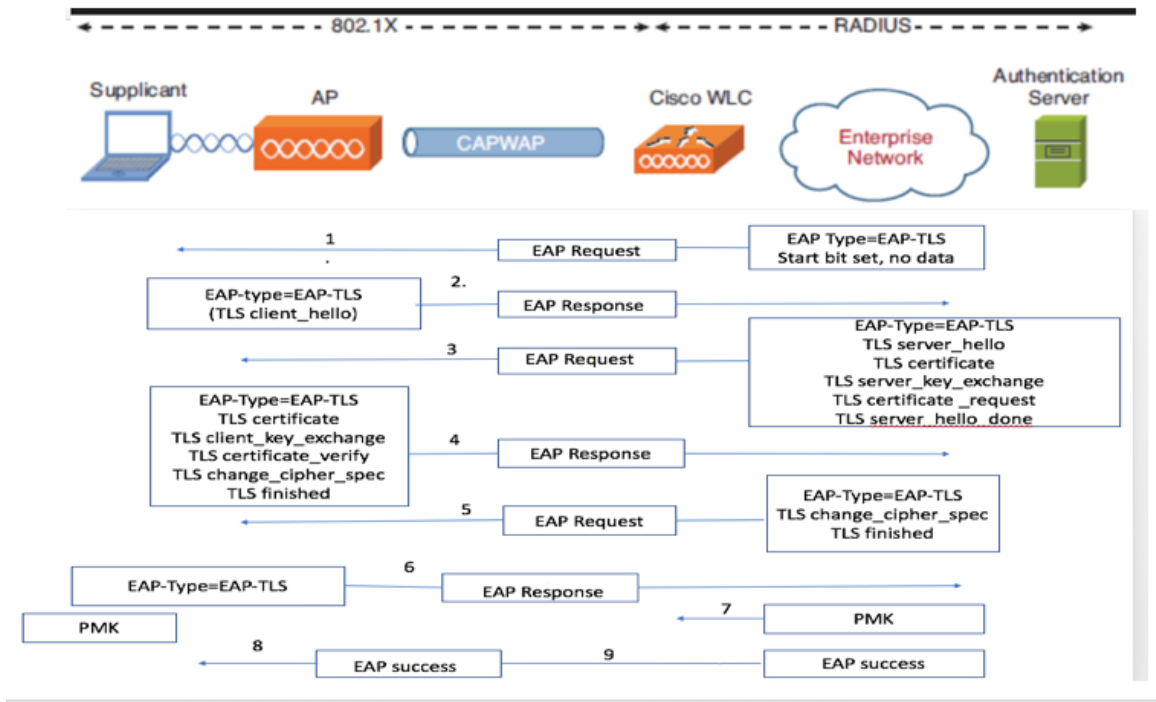
Using tools like eaphammer (<https://github.com/s0lst1c3/eaphammer/>), an attacker can attempt to negotiate the weakest possible EAP type and capture credentials with GTC or hashed credentials with MSCHAPv2.

## INCREASING DETECTION RECOMMENDATIONS

When configuring a Wireless IDS, consider these recommendations: <https://solstice.sh/2019/11/22/modern-wireless-tradecraft-pt-iv-tradecraft-and-defensive-strategy/>

## USE EAP TYPES WITH MUTUAL AUTHENTICATION TO LIMIT ATTACKS

EAP-TLS is the oldest and most well-known protocol for mutually authenticating devices. This configuration flow shows the Cisco WLC setup for mutual authentication using EAP-TLS.



Cisco Documentation For Using WLC for EAP-TLS <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/213543-configure-eap-tls-flow-with-ise.html>

This system relies on the internal certificate authority (CA) used on the infrastructure’s RADIUS server. When moving from password-based authentication to mutual certificate authentication, it is often possible to leverage the existing RADIUS server deployment.

- Cisco ISE: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-ise.html>
- Microsoft NPS: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/certificate-requirements-eap-tls-peap>
- Freeradius: [https://documentation.meraki.com/MR/Encryption\\_and\\_Authentication/Freeradius%3A\\_Configure\\_freeradius\\_to\\_work\\_with\\_EAP-TLS\\_authentication](https://documentation.meraki.com/MR/Encryption_and_Authentication/Freeradius%3A_Configure_freeradius_to_work_with_EAP-TLS_authentication)

## Appendix B: Wireless Penetration Test Methodology

### WIRELESS NETWORK ENUMERATION

During the enumeration phase Cisco catalogs the wireless networks in the target facility, their configurations, and any associated clients. When on-site, Cisco conducts walk-arounds of facilities to attempted to identify unmanaged or rogue access points. Tools that may be used in this phase can include:

- Airodump-ng - <https://www.aircrack-ng.org/>
- Kismet - <https://www.kismetwireless.net/>

### DIRECT EVALUATION OF WIRELESS NETWORKS

Cisco attempts direct attacks against wireless network infrastructure: attempting PMKID extraction, capturing WPA 4-way handshakes, attempting de-authentication of clients, etc. In addition, Cisco may also examine the segmentation and configuration of guest networks. Tools that may be used in this phase can include:

- Aircrack-ng suite of tools - <https://www.aircrack-ng.org/>
- KRACK test scripts - <https://github.com/vanhoefm/krackattacks-scripts>
- Nmap - <https://nmap.org/>

### ROGUE ACCESS POINT ATTACKS AGAINST WIRELESS CLIENTS

Cisco sets up malicious access points to attempt to capture use credentials. Tools that may be used in this phase can include:

- Hostapd-wpe - <https://github.com/OpenSecurityResearch/hostapd-wpe>
- eaphammer - <https://github.com/s0lst1c3/eaphammer>
- WiFi Pineapple or other Dropboxes - <https://shop.hak5.org/products/wifi-pineapple>

## Appendix C: CVSS Vector Strings

### WIRELESS PENETRATION TEST

#### 4.1 Weak Pre-Shared Keys In Use

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L/E:H/RL:O/RC:C

#### 4.2 Default Device Credentials In Use

AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

#### 4.3 Open Wireless Networks In Use

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

#### 4.4 PEAP Vulnerable To "Rogue AP" Attacks

AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C

#### 4.5 Client Configuration Does Not Define RADIUS Certificate CommonName

AV:A/AC:L/PR:N/C:H/I:L/A:N/S:U/UI:N

#### 4.6 Admin Interfaces Presented To Guest Wireless Network

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

#### 4.7 MAC Spoofing Allows Guest Network Access

AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

#### 4.8 Access Points Using WiFi Protected Setup (WPS)

AV:N/AC:L/PR:N/C:L/I:L/A:L/S:U/UI:N/E:F/RL:O/RC:U

#### 4.9 Access Points Allow PMKID Extraction

AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N/E:H/RL:O/RC:C

#### 4.10 WPA2-PSK Allows Handshake Collection

AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:W/RC:C

#### 4.11 Gratuitous Information Disclosed Within DNS Server Responses

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

#### 4.12 Wireless Client Isolation Not Enabled

AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

#### 4.13 Internet-Based DNS Queries Allowed Prior To Authorization

AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:H/RL:O/RC:C



## Appendix D: Definition of Terms

Each finding identified during the assessment is allocated a Severity Level and CVSS 3.0 score; the Severity Level being directly derived from the CVSS 3.0 score as per the standard, as well as being described under the Specific Details, Security Impact and Recommendations headings, with an additional Steps to Reproduce header, where applicable. The ratings are based on the individual objective finding and not the subjective risk the issue may pose.

### CVSS

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS consists of 3 groups: Base, Temporal and Environmental.

Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics. These metric groups are described as follows:

- Base: represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and across user environments.
- Temporal: represents the characteristics of a vulnerability that may change over time but not across user environments.
- Environmental: represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

Cisco uses the CVSS 3.0 scoring mechanism and directly maps those to severity ratings for each finding, as defined in the CVSS 3.0 standard shown below:

Severity Rating	CVSS Score
Critical	9.0 – 10.00
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
None	0.0

## CWE

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

Cisco applies a relevant CWE against each finding in order to allow for finding grouping, which is then used to generate the remediation action plan in the recommendations section of the report.

**Americas Headquarters**

Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**

Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**

Cisco Systems International BV Amsterdam,  
The Netherlands

---

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



## DESCRIPTIONS (Continued from Page 1)

EPLI= Employment Practices Liability Insurance

**ADDENDUM ACKNOWLEDGEMENT FORM**

**SOLICITATION NO.:** ~~ARFQ LOT 24-08~~

*CRFQ LOT...09*

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**

(Check the box next to each addendum received)

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6  |
| <input type="checkbox"/> Addendum No. 2            | <input type="checkbox"/> Addendum No. 7  |
| <input type="checkbox"/> Addendum No. 3            | <input type="checkbox"/> Addendum No. 8  |
| <input type="checkbox"/> Addendum No. 4            | <input type="checkbox"/> Addendum No. 9  |
| <input type="checkbox"/> Addendum No. 5            | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Networking For Future (NFF), Inc.

Company

*Kevin J Reith*

Authorized Signature

~~2/12/2024~~ 3/28/2024

Date

**NOTE:** This addendum acknowledgement should be submitted with the bid to expedite document processing.