National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Systems, Inc. IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2

Report Number:	**CCEVS-VR-10907-2018**
Dated:	**11/29/2018**
Version:	**0.3**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
Meredith Hennan
The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in December 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018.

The Target of Evaluation (TOE) is the Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 Common Criteria Security Target, version 1.0, 11/16/2018 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018
ST	Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 Security Target, version 1.0, 11/16/2018
Evaluation Technical Report	Evaluation Technical Report for Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2, version 1.0, 11/19/2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Jerome Myers, Meredith Hennan

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is the Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2. The TOE is comprised of both software and hardware. The hardware is comprised of the IE2000 Series, IE4000 Series, IE5000 Series and 2500 Series CGS models. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS 15.2.

The Cisco IE2K, IE4K, IE5K and CGS that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The Cisco IE2K, IE4K, IE5K and CGS primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation.
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program).
- USB port (v2.0) (note, USB devices are outside the scope of the evaluation).
    - Type A for Storage, all Cisco supported USB flash drives.
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.
- Non-volatile random-access memory (NVRAM) is used to store router configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100/1000 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

3.1 TOE Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The Cisco IE2K, IE4K, IE5K and CGS are switching and routing platforms that provide connectivity and security services onto a single, secure device. These switches offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers.

The Cisco IE2K, IE4K, IE5K and CGS are single-device security and switching solutions for protecting the network.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The TOE is a hardware and software solution composed of the switch models IE2000 Series, IE4000 Series, IE5000 Series and 2500 Series CGS running Cisco IOS 15.2:

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target.

IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators.
Management Workstation	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 secured connection. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages over IPsec.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.

The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS configuration determines how packets are handled to and from the TOE's network interfaces. If the Cisco IE2K, IE4K, IE5K and CGS is to be remotely administered, then the management station must be connected to an internal network, SSHv2 may be used to connect to the switch. A syslog server is also used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication

4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The Cisco IE2K, IE4K, IE5K and CGS provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections;
- modifications to the group of users that are part of the authorized administrator roles;
- all use of the user identification mechanism;
- any use of the authentication mechanism;
- Administrator lockout due to excessive authentication failures;
- any change in the configuration of the TOE;
- changes to time;
- initiation of TOE update;
- indication of completion of TSF self-test;
- maximum sessions being exceeded;
- termination of a remote session;
- attempts to unlock a termination session and
- initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE can be configured to block new permit actions.

The audit logs can be viewed on the TOE using the appropriate IOS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.

4.2 Cryptographic support

The TOE provides cryptography in support of other Cisco IE2K, IE4K, IE5K and CGS security functionality. This IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) certificate 2388 and has been validated for conformance to the requirements of FIPS 140-2 Level 1.

The TOE provides cryptography in support of remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The cryptographic services provided by the TOE are described in the table below.

TOE Provided Cryptography

Cryptographic Method	Use within the TOE
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.
HMAC	Used for keyed hash, integrity services in SSH session establishment.
DH	Used as the Key exchange method for SSH
Internet Key Exchange	Used to establish initial IPsec session.
KAS	Used to provide key exchange method
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing.
SP 800-90A DRBG	Used for random number generation, key generation and seeds to asymmetric key generation Used in IPsec session establishment. Used in SSH session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification

4.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSHv2 secured connection. The TOE supports use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of authentication attempts fail has exceeded the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec.

4.4 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 secured connection with the TOE acting as SSH server or via a local console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely;
- Configuration of warning and consent access banners;
- Configuration of session inactivity thresholds;
- Updates of the TOE software;
- Configuration of authentication failures;
- Configuration of the audit functions of the TOE;
- Configuration of the TOE provided services; and
- Configuration of the cryptographic functionality of the TOE.

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. The privileged administrator is the Authorized Administrator of the TOE who has the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE.

4.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS is not a general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4.6 TOE access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

4.7 Trusted path/channels

The TOE allows trusted channels to be established to itself from remote administrators that is SSHv2 secured connection, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018

That information has not been reproduced here and the NDcPP20E should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP20E as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).

- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. The security claims focus on the TOE as a secure network infrastructure device and do not focus on other key functions provided by the TOE, such as controlling the flow of network packets among the attached networks. These functions can be used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

6 Documentation

The following document was made available with the TOE for evaluation and is the only documentation that should be trusted for administration or use of the TOE in its evaluated configuration:

- Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0, 11/16/2018

7 IT Product Testing

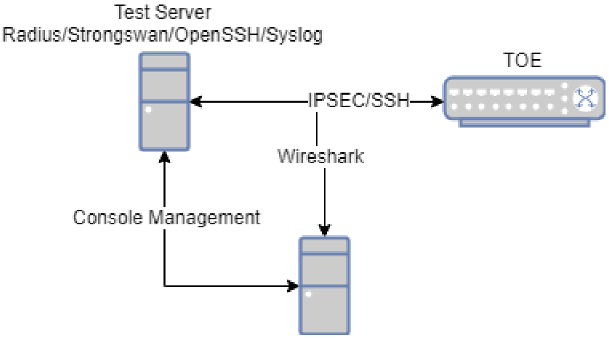
This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP20E) for Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2, Version 1.0, 11/19/2018 (AAR).

7.1 Test Software

- Ubuntu 16.04
- FreeRadius 3.0.5
- Strongswan 5.3.5
- OpenSSH 7.2p2
- Windows 10 Enterprise

- Wireshark v2.4.2
- Putty v0.68

7.2 Test Environment



7.3 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.4 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP20E including the tests associated with optional requirements.

8 Evaluated Configuration

The TOE is the Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2. The TOE is comprised of both software and hardware which must be configured in accordance with the documentation listed in Section 6.

The hardware is comprised of the following IE2000 Series, IE4000 Series, IE5000 Series and 2500 Series CGS models:

IE2000 Series

- IE-2000-4TS-L, IE-2000-4TS-B, IE-2000-4T-L, IE-2000-4T-B, IE-2000-4TS-G-L, IE-2000-4TS-G-B, IE-2000-4T-G-L, IE-2000-4T-G-B, IE-2000-4S-TS-G-L, IE-2000-4S-TS-G-B, IE-2000-8TC-L, IE-2000-8TC-B, IE-2000-8TC-G-L, IE-2000-8TC-G-B, IE-2000-8TC-G-E, IE-2000-16TC-L, IE-2000-16TC-B, IE-2000-16TC-G-L, IE-2000-16TC-G-E, IE-2000-16TC-G-X, IE-2000-8TC-G-N, IE-2000-16TC-G-N, IE-2000-16PTC-G-L, IE-2000-16PTC-G-E, IE-2000-16PTC-G-NX

IE4000 Series

- IE-4000-4TC4G-E, IE-4000-8S4G-E, IE-4000-4T4P4G-E, IE-4000-16T4G-E, IE-4000-4S8P4G-E, IE-4000-8GT4G-E, IE-4000-8GS4G-E, IE-4000-4GC4GP4G-E, IE-4000-

16GT4G-E, IE-4000-8GT8GP4G-E, IE-4000-4GS8GP4G-E, IE-4010-16S12P, IE-4010-4S24P

IE5000 Series

- IE-5000-12S12P-10G, IE-5000-16S12P

2500 Series CGS

- CGS-2520-24TC, CGS-2520-16S-8PC

The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS 15.2.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP20E.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP20E related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP20E and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

On 10/02/2018 the evaluator searched the following sources for vulnerabilities:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)

- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

Each site was searched using the following terms:

1. TCP
2. IPsec
3. SSH
4. Switch
5. Router
6. Cisco
7. IoT

On 11/19/2018 a second public vulnerability search was performed using the same sources and terms from 10/1/2018 to present to ensure the most recently published vulnerabilities were included.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All validator comments have been addressed in Section 5, Assumptions and Clarification of Scope.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 Common Criteria Security Target, Version 1.0, 11/16/2018.*

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018.

[5] Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2 Common Criteria Security Target, Version 1.0, 11/16/2018 (ST).

[6] Assurance Activity Report (NDcPP20E) for Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2, Version 1.0, 11/19/2018 (AAR).

[7] Detailed Test Report (NDcPP20E) for Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2, Version 1.0, 11/19/2018 (DTR).

[8] Evaluation Technical Report for Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS 15.2, Version 1.0, 11/19/2018 (ETR)