National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Crestron DigitalMedia NVX® AV-over-IP v5.2

Report Number: CCEVS-VR-11215-2022
Dated: 16 February 2022
Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
John Butterworth
Jenn Dotson
Lisa Mitchell
Linda Morrison

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Crestron DigitalMedia NVX® AV-over-IP v5.2 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation of Crestron DigitalMedia NVX® AV-over-IP v5.2 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in February 2022. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, and assurance activities specified in the Supporting Document Mandatory Technical Document *Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 [cPPND]. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The TOE is a series of audio & video (AV) over IP network devices that encrypt, decrypt and transmit HDMI video, USB and analog audio data over customer networks. These communication streams use an AES-based HDCP standard that is not covered by the [cPPND] and therefore is not evaluated. The focus of this evaluation is on the TOE functionality supporting the claims in the collaborative Protection Profile for Network Devices ([cPPND].

The security functionality specified in [cPPND] includes protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and use of NIST-validated cryptographic mechanisms. The [cPPND] does not define requirements for encryption of audio and video so the TOE focuses on the security of the network channels used for syslog, management, and authentication.

The Leidos evaluation team determined that the TOE is conformant to *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in Crestron DigitalMedia NVX® AV-over-IP v5.2 Security Target, Version 1.0, 15 February 2022. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test reports. The validation team found that the evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020, and that the assurance activities specified in the Supporting Document had been performed appropriately. 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.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Crestron DigitalMedia NVX® AV-over-IP v5.2
Security Target	Crestron DigitalMedia NVX® AV-over-IP v5.2 Security Target, Version 1.0, 15 February 2022
Sponsor & Developer	Crestron Electronics, Inc. 15 Volvo Drive Rockleigh, New Jersey 07647
Completion Date	February 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant
CCTL	Leidos 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Leidos: Pascal Patin, Anthony Apted, Greg Beaver
Validation Personnel	MITRE: Paul Bicknell, John Butterworth, Jenn Dotson, Lisa Mitchell, Linda Morrison

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the Crestron DigitalMedia NVX® AV-over-IP v5.2 Security Target and Final Evaluation Technical Report (ETR).

3.1 Security Audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log and export them to a syslog server using a TLS protected channel.

3.2 Cryptographic Support

The TOE provides CAVP certified cryptography in support of its SSH, TLS, and NTP implementations and for verifying TOE update package signatures. Cryptographic services include key management, random bit generation, symmetric encryption and decryption, digital signature, and secure hashing.

3.3 Identification and Authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. The TOE authenticates a user's credentials (password, key) using a local mechanism provided by the TOE. The TOE also provides X.509 certificate checking for its TLS connections.

3.4 Security Management

The TOE provides CLI and web-based management interfaces that an administrator can access remotely via a network port. The CLI can also be accessed locally by directly connecting to a network port and using SSH. Remote connections to the management interface are protected with SSH for the CLI and HTTPS for the GUI. The management interface is limited to the authorized administrator.

3.5 Protection of the TSF

The TOE implements various self-protection mechanisms. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It relies upon either manually provided time or an NTP server in its environment to ensure reliable timestamps. It protects sensitive data such as passwords and cryptographic keys stored on the TOE's internal Flash so that they are not accessible even by an authorized administrator.

3.6 TOE Access

The TOE will terminate local and remote interactive sessions after a configurable period of inactivity. The TOE additionally provides the capability for administrators to terminate their own interactive sessions. The TOE can be configured to display an advisory and consent warning message before establishing a user session.

3.7 Trusted Path/Channels

The TOE provides local administration which is subject to physical protection. To access the TOE locally, an administrator must directly connect their workstation to a network port and use SSH and successfully login. When accessed remotely, the CLI and GUI management interfaces are protected by SSH and TLS respectively, thus ensuring protection against modification and disclosure.

The TOE protects communications with the external syslog servers from modification and disclosure by using TLS.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 [CPPND]

That information has not been reproduced here and [cPPND] should be consulted if there is interest in that material.

4.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in [cPPND] 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.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 *collaborative Protection Profile for Network Devices* and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Crestron DigitalMedia NVX® AV-over-IP v5.2 Security Target*, Version 1.0, 15 February 2022. Any additional security related functional capabilities of the product were not covered by this evaluation.
- 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 TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- The TOE must be installed, configured and managed as described in the following guidance documents included in the evaluated configuration:
    a. Crestron DigitalMedia NVX Series v5.2 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0
    b. DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)
    c. DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)
    d. DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc.8906A)
    e. DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)
    f. DM-NVX-D80-IOAV Quick Start (Doc. 8526A)
    g. DM-NVX-363 and DM-NVX-360 Quick Start (Doc. 8634)
    h. DM-NVX-363C and DM-NVX-360C Quick Start (Doc. 8636)
    i. DM-NVX-E760 Quick Start (Doc. 8646B)
    j. DM-NVX-E760C Quick Start (Doc. 8638B).

5 Architectural Information

The Target of Evaluation (TOE) is identified as the Crestron DigitalMedia NVX® AV-over-IP v5.2. The TOE includes each of the following appliance models, each with firmware version 5.2.4651.00030:

- DM-NVX-350
- DM-NVX-350C
- DM-NVX-351
- DM-NVX-351C
- DM-NVX-352
- DM-NVX-352C
- DM-NVX-E30
- DM-NVX-E30C
- DM-NVX-D30
- DM-NVX-D30C
- DM-NVX-D80-IOAV
- DM-NVX-363
- DM-NVX-363C
- DM-NVX-E760
- DM-NVX-E760C

The TOE is a digital video and audio distribution network device that switches 4K video sources and displays at 60 frames per second (fps) with full 4:4:4 color sampling, High Dynamic Range (HDR) video support, standard 1-Gigabit Ethernet infrastructure, and Pixel Perfect Processing technology to provide video transport in all applications. A video signal is encoded and decoded to achieve imperceptible end-to-end latency of less than 1 frame. The image quality of the source is maintained across a 1-Gigabit network at any resolution up to 4K60 4:4:4. The digital video and audio transport and encoding/decoding are not evaluated.

For the purpose of this evaluation, the TOE is treated as a network device offering NIST validated cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to export audit records), protected using HTTPS/TLS and SSH.

Cryptographic functionality is performed by the TOE's '*Crestron Crypto Kernel for Open SSL*' software module that includes third-party SafeLogic OpenSSL in support of higher level protocols (TLS, SSH). The module's FIPS-Approved cryptographic algorithms have obtained CAVP certificates.

The TOE audits security relevant events, stores audit records locally, and can be configured to forward its audit records to an external syslog server in the network environment. An administrator can configure the TOE to solicit time from an NTP server, and alternatively the administrator can manually set the TOE's time.

The TOE uses TLS to protect syslog, offers a management GUI protected by TLS/HTTPS, and provides a management Command Line Interface (CLI) protected by SSH.

Administrators are able to query the current version of the product firmware and manage the security functions of the TOE, including performing updates on the product. Public/private keys are used to provide digital signatures for protection of the update files.

The TOE provides self-tests to ensure the integrity and correct operation of the TOE.

6 Documentation

Creston Electronics provides a set of documentation for the end users of the TOE, providing guidance on the installation, configuration and use of the TOE. The following documents were specifically examined in the context of the evaluation:

- Crestron DigitalMedia NVX Series v5.2 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0
- DM-NVX-350, DM-NVX-351, and DM-NVX-352 Quick Start (Doc.8391C)
- DM-NVX-350C, DM-NVX-351C, and DM-NVX-352C Quick Start (Doc. 8392B)
- DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc.8906A)
- DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)
- DM-NVX-D80-IOAV Quick Start (Doc. 8526A)
- DM-NVX-363 and DM-NVX-360 Quick Start (Doc. 8634)
- DM-NVX-363C and DM-NVX-360C Quick Start (Doc. 8636)
- DM-NVX-E760 Quick Start (Doc. 8646B)
- DM-NVX-E760C Quick Start (Doc. 8638B)

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the proprietary Crestron_NVX Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.2, 11 February 2022, as characterized in the publicly available Assurance Activities Report For Crestron DigitalMedia NVX® AV-over-IP v5.2.

7.1 Developer Testing

The assurance activities in *Evaluation Activities for Network Device cPP* do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the Test Assurance Activities specified in *Evaluation Activities for Network Device cPP*. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report identified above.

Testing of the TOE was performed at the Leidos Accredited Testing and Evaluation Lab located in Columbia, Maryland from January, 2021 to November, 2021. For the purposes of that testing, the configuration depicted in Figure 1 was used as a basis for testing.

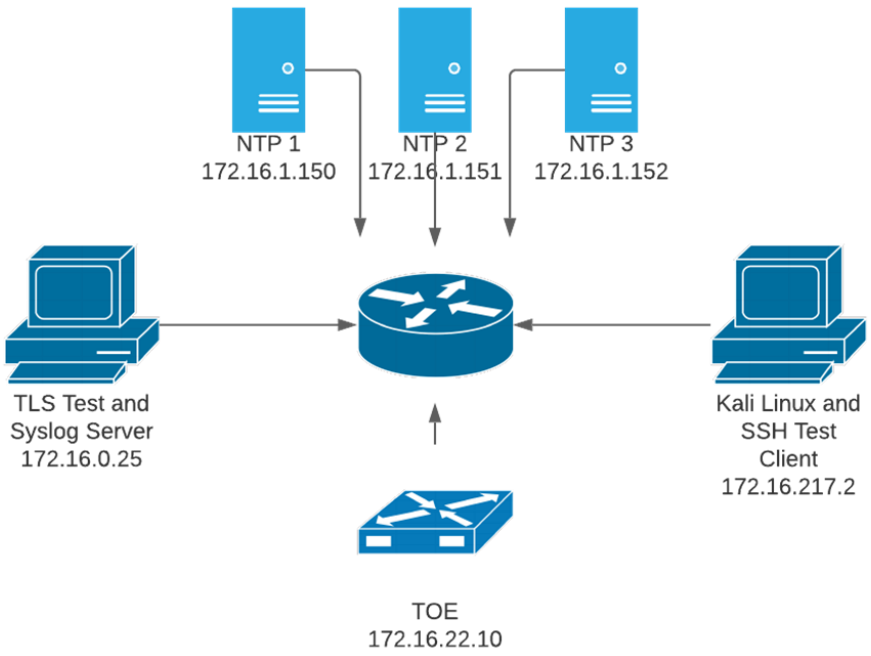

Figure 1: Physical Devices Configuration

NTP 1, NTP 2, NTP 3
Ubuntu 18.04 running ntpd 4.2.8p10

TLS Test and Syslog Server
Ubuntu 18.04
Wireshark 2.6.10
Python
Leidos Proprietary TLS tools

Kali Linux and SSH Test Client
Kali Linux Release 2020.4
Wireshark 2.6.10
XCA Certificate Authority 2.0.1
SSLyze 2.1.4

Tested TOE Model
DM-NVX-363

The evaluation team followed the installation and configuration procedures documented in the product guidance to install the TOE in the test environment.

Subsequently, the evaluators exercised all the test cases. The tests were selected in order to ensure that each of the test assertions specified in *Evaluation Activities for Network Device cPP* were covered. All tests passed. A summary of the testing performed by the evaluation team is provided in *Assurance Activities Report For Crestron DigitalMedia NVX® AV-over-IP v5.2*.

7.3 Test Equivalence Rationale

The evaluated configuration comprises Crestron DigitalMedia NVX® AV-over-IP v5.2, with firmware version 5.2.4651.00030, comprising the following appliance models:

- DM-NVX-350
- DM-NVX-350C
- DM-NVX-351
- DM-NVX-351C
- DM-NVX-352
- DM-NVX-352C
- DM-NVX-E30
- DM-NVX-E30C
- DM-NVX-D30
- DM-NVX-D30C
- DM-NVX-D80-IOAV
- DM-NVX-363
- DM-NVX-363C
- DM-NVX-E760
- DM-NVX-E760C

Each appliance contains an Intel Arria 10 SX SoC FPGA that includes an ARM Cortex-A9 MPCore processor implementing the ARMv7-A microarchitecture, and an Angstrom Linux v2014.12 operating system, that uses version 4.19 of the Linux kernel. The "C" indicated in the above appliance models is a form factor with a chassis card.

The NVX Models differ in terms of form factor, function (sender, receiver), number and types of external control and data ports and maximum Input/Output resolution. The NVX models use the same firmware image files and provide equivalent security-relevant functionality. There are no security relevant differences between the appliance models.

The DM-NVX-363 TOE appliance was tested in the evaluated configuration. Since the NVX models use the same firmware image files and provide equivalent security-relevant functionality, they can be considered equivalent.

7.4 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

8 Evaluated Configuration

The Target of Evaluation (TOE) is identified as the Crestron DigitalMedia NVX® AV-over-IP v5.2. The TOE includes each of the following appliance models, each with firmware version 5.2.4651.00030:

- DM-NVX-350
- DM-NVX-350C
- DM-NVX-351
- DM-NVX-351C
- DM-NVX-352
- DM-NVX-352C
- DM-NVX-E30
- DM-NVX-E30C
- DM-NVX-D30
- DM-NVX-D30C
- DM-NVX-D80-IOAV
- DM-NVX-363
- DM-NVX-363C
- DM-NVX-E760
- DM-NVX-E760C.

The TOE is installed and configured according to the product installation guidance identified in Section 6.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.2e, 23 March 2020, in conjunction with Version 3.1, Revision 5 of the CC and CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: Evaluated Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is the Crestron DigitalMedia NVX® AV-over-IP v5.2 Security Target, Version 1.0, 15 February 2022.

13 Abbreviations and Acronyms

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol—a means of synchronizing clocks over a computer network
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 1: Introduction and general model.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 2: Security functional components.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017. Part 3: Security assurance components.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, 5, April 2017. Evaluation methodology.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Crestron DigitalMedia NVX® AV-over-IP v5.2 Security Target, Version 1.0, 15 February 2022.

[7] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[8] Evaluation Technical Report for Crestron DigitalMedia NVX® AV-over-IP v5.2 (Proprietary), Version 1.0, 16 February 2022.

[9] Assurance Activities Report for Crestron DigitalMedia NVX® AV-over-IP v5.2, Version 1.0, 16 February 2022.

[10] Crestron_NVX Common Criteria Test Report and Procedures For Network Device collaborative PP, Version 2.2e, Version 1.2, 11 February 2022.