National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Crestron DigitalMedia NVX®AV-over-IP v7.1

Report Number: CCEVS-VR-VID11471-2024
Dated: 9 October 2024
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

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Josh Marciante
Pascal Patin
Kevin Zhang
Leidos Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Security Policy 4
3.1 Security Audit 4
3.2 Cryptographic Support 4
3.3 Identification and Authentication 4
3.4 Security Management 4
3.5 Protection of the TSF 4
3.6 TOE Access 4
3.7 Trusted Path/Channels 4
4 Assumptions and Clarification of Scope 5
4.1 Assumptions 5
4.2 Clarification of Scope 5
5 Architectural Information 6
6 Documentation 7
7 IT Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 8
8 Evaluated Configuration 9
9 Results of the Evaluation 10
9.1 Evaluation of the Security Target (ASE) 10
9.2 Evaluation of the Development (ADV) 10
9.3 Evaluation of the Guidance Documents (AGD) 10
9.4 Evaluation of the Life Cycle Support Activities (ALC) 10
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 11
9.6 Vulnerability Assessment Activity (VAN) 11
9.7 Summary of Evaluation Results 12
10 Validator Comments/Recommendations 13
11 Annexes 14
12 Security Target 15
13 Abbreviations and Acronyms 16
14 Bibliography 17

List of Tables

Table 1: Evaluation Identifiers 2

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of the Crestron DigitalMedia NVX®AV-over-IP v7.1 provided by Creston Electronics, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of Crestron DigitalMedia NVX®AV-over-IP v7.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in October 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Leidos. 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 2.2e, 23 March 2020 (NDcPP22e).

The TOE is the Crestron DigitalMedia NVX®AV-over-IP v7.1. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Crestron DigitalMedia NVX® AV-over-IP v7.1 Security Target*, Version 1.0, October 3, 2024, 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

Evaluation Scheme:	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product (TOE):	Crestron DigitalMedia NVX® AV-over-IP v7.1
Sponsor:	Crestron Electronics, Inc. 15 Volvo Drive Rockleigh, New Jersey 07647
Developer:	Crestron Electronics, Inc. 15 Volvo Drive Rockleigh, New Jersey 07647
CCTL:	Leidos 6841 Benjamin Franklin Drive Columbia, MD 21046
ETR:	*Evaluation Technical Report for Crestron DigitalMedia NVX®AV-over-IP v7.1*, Version 1.2, 7 October 2024
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Conformance Result:	CC Part 2 extended, CC Part 3 conformant
Security Target:	*Crestron DigitalMedia NVX® AV-over-IP v7.1 Security Target*, Version 1.0, October 3, 2024

Protection Profile:	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Evaluation Personnel:	Leidos: Josh Marciante, Kevin Zhang, Pascal Patin
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Randy Heimann, Lori Sarem

3 Security Policy

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

Note: The description of the security policy has been derived from the *Crestron DigitalMedia NVX®AV-over-IP v7.1 Security Target*.

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 [NDcPP22e]

That information has not been reproduced here and the NDcPP22e 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 the NDcPP22e as described for this TOE in the ST. 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 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 NDcPP22e 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 NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

5 Architectural Information

The Target of Evaluation (TOE) is identified as the Crestron DigitalMedia NVX®AV-over-IP v7.1. The TOE includes the following appliance models, each with firmware version 7.1.5259.00081:

- DM-NVX-E10
- DM-NVX-E20
- DM-NVX-E20-2G
- DM-NVX-E30
- DM-NVX-E30C
- DM-NVX-E760
- DM-NVX-E760C
- DM-NVX-D10
- DM-NVX-D20
- DM-NVX-D30
- DM-NVX-D30C
- DM-NVX-D200
- DM-NVX-D80-IOAV
- DM-NVX-350
- DM-NVX-350C
- DM-NVX-351
- DM-NVX-351C
- DM-NVX-352
- DM-NVX-352C
- DM-NVX-360
- DM-NVX-360C
- DM-NVX-363
- DM-NVX-363C.

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.

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®AV-over-IP v7.1 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, October 4, 2024
- 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-E10 and DM-NVX-D10 Quick Start (Doc. 9001A)
- DM-NVX-E20 and DM-NVX-D20 Quick Start (Doc. 9000A)
- DM-NVX-E20-2G Quick Start (Doc. 9160A)
- DM-NVX-E30 and DM-NVX-D30 Quick Start (Doc.8906B)
- DM-NVX-E30C/DM-NVX-D30C Quick Start (Doc. 8346A)
- DM-NVX-D80-IOAV Quick Start (Doc. 8526A)
- DM-NVX-D200 Quick Start (Doc. 9091A)
- DM-NVX-363 and DM-NVX-360 Quick Start (Doc. 8634B)
- DM-NVX-363C and DM-NVX-360C Quick Start (Doc. 8636A)
- DM-NVX-E760 Quick Start (Doc. 8646B)
- DM-NVX-E760C Quick Start (Doc. 8638B).

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

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 proprietary *Crestron DigitalMedia NVX®AV-over-IP v7.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e,* Version 1.0, October 4, 2024 (DTR), as characterized in the publicly available *Assurance Activities Report For Crestron DigitalMedia NVX®AV-over-IP v7.1*, Version 1.1, October 4, 2024.

7.1 Developer Testing

The assurance activities 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 DTR identified above.

Testing of the TOE was performed at the Leidos Accredited Testing and Evaluation Lab located in Columbia, Maryland from February 2024 to October 2024.

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

Subsequently, the Evaluation team 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 the AAR.

8 Evaluated Configuration

See Section 5 for the Evaluated Configuration.

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 5 and CEM version 3.1 rev 5. The evaluation determined the Crestron DigitalMedia NVX®AV-over-IP v7.1 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

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 Crestron DigitalMedia NVX®AV-over-IP v7.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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 ST and Guidance document. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

The Validation team 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. The guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team 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 Validation team 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 NDcPP22e and recorded the results in the DTR, summarized in the AAR.

The Validation team 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 contained in the AVA report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the following sites:

- National Vulnerability Database (https://nvd.nist.gov/).
- Crestron Security Advisories (https://www.crestron.com/Security#securityAdvisoriesTab).

The final search was conducted October 3, 2024, with the following search terms:

- Crestron
- Crestron DM-NVX
- DM-NVX-350
- DM-NVX-350C
- DM-NVX-351
- DM-NVX-351C
- DM-NVX-352
- DM-NVX-352C
- DM-NVX-360
- DM-NVX-360C
- DM-NVX-363
- DM-NVX-363C
- DM-NVX-E10
- DM-NVX-E20
- DM-NVX-E20-2G
- DM-NVX-E30C
- DM-NVX-E30
- DM-NVX-D10
- DM-NVX-D20
- DM-NVX-D30
- DM-NVX-D30C
- DM-NVX-D80-IOAV
- DM-NVX-D200
- DM-NVX-E760
- DM-NVX-E760C
- Intel Arria 10 SX SoC FPGA
- ARM Cortex-A9 MPCore
- Lighttpd 1.4.52
- Redis v5.0.14

- openbsd openssh 9.8p1
- Net-SNMP 5.9.4
- OpenSSL 1.0.2zd
- NTPSec 1.2.3
- Angstrom Linux
- Crestron AV Router.

The Validation team 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

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Crestron DigitalMedia NVX®AV-over-IP v7.1 Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, October 4, 2024, and the associated Quick Start documents listed in Section 6. As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE, either earlier or later, were evaluated. Any additional customer documentation, not listed in Section 6, provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

The Validation team suggests 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 ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

11 Annexes

Not applicable.

12 Security Target

Crestron DigitalMedia NVX® AV-over-IP v7.1 Security Target, Version 1.0, October 3, 2024.

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

[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 v7.1 Security Target*, Version 1.0, October 3, 2024.

[8] *Evaluation Technical Report for Crestron DigitalMedia NVX®AV-over-IP v7.1* (Proprietary), Version 1.2, 7 October 2024

[9] *Assurance Activities Report For Crestron DigitalMedia NVX®AV-over-IP v7.1,* Version 1.1, 4 October 2024.

[10] *Crestron DigitalMedia NVX®AV-over-IP v7.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e*, Version 1.0, October 4, 2024.

[11] *Crestron DigitalMedia NVX® AV-over-IP v7.1 Vulnerability Assessment*, Version 1.0, October 4, 2024.