ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Crestron DigitalMedia NVX®AV-over-IP v5.2

Crestron DigitalMedia NVX®AV-over-IP

Maintenance Report Number: CCEVS-VR-VID11215-2022

Date of Activity: 11 April 2022

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Cisco Network Convergence System 1000 Series Impact Analysis Report, Version 1.1, 1 September 2020
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

Assurance Continuity Maintenance Report:

Crestron Electronics, Inc., submitted an Impact Analysis Report (IAR) for the "Crestron DigitalMedia NVX®AV-over-IP v5.2" to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 6 April 2022. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consisted of the Security Target (ST), the Operational User Guide, and the Impact Analysis Report (IAR). The ST and User Guide were updated, and the IAR was new.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Crestron Electronics, Inc. Products Security Target, Version 1.1, 4/6/2022	The ST was updated to include 2 additional appliance models and the tested firmware version number.
Guidance: Crestron Common Criteria Supplement, Version 1.1	The guidance document was updated to include 2 additional models and the tested firmware version number in the initial

	Introduction and the referenced Installation Guidance section.

Changes to the TOE:

Each of the changes to "Crestron DigitalMedia NVX®AV-over-IP v5.2" fell into the following categorization:

Major Changes

None.

Minor Changes

The TOE was revised with the following changes but remains Crestron DigitalMedia NVX®AV-over-IP v5.2.

1 Hardware changes – The DM-NVX-360 and DM-NVX-360C models were added to the list of appliance models. They are essentially identical to the previously evaluated CM-NVX-363 and DN-NVX-363C models with the exception that certain audio processing hardware was removed. The NVX models all use the same firmware image files and provide equivalent security-relevant functionality. There are no security relevant differences between any of the appliance models.
2 The product firmware version was updated from: 5.2.4651.00030 to 5.2.4651.00032.

Product Firmware Changes	**Assessment/Impact**
SafeLogic OpenSSL was updated from version 1.0.2x to version 1.0.2zd	The underlying FIPS module was unchanged and so CAVP certification was unaffected
Software vulnerabilities were resolved.	• CVE-2021-23840 which affects all encryption/decryption; • CVE-2021-23841, CVE-2021-3712, CVE-2022-0778 which all are related to reading certificate information; and • CVE-2021-4160, CVE-2021-23839 are related to features not related to the TOE.
Link Layer Discovery Protocol (LLDP) Power over Ethernet (PoE) negotiation was modified to prevent startup problems with certain non-conforming switches.	This Layer 2 Ethernet functionality is used for basic hardware negotiation and so has no security relevant functionality.
Coredump information was minimized to avoid SDCARD overuse.	This change has no security relevant functionality

Regression Testing:

Crestron's internal security team performed regression testing including, but not limited to, the following:

- Tested Certificate extensions including extendedKeyUsage and basicConstraints,
- Tested Certificate ealidation and rejection including CN, SAN and wildcard certificates,
- Tested connection to RSYSLOG
    - Validation of trusted certificate chain
    - Validation of TLS ciphers,
- Tested SCIP Communication
    - Validation of trusted certificate chain
    - Validation of TLS ciphers,
- Tested OCSP including both online servers and stapled responses,
- Tested certificates with various algorithms,
- Tested Certificate Signing Request handling,
- Reviewed audit logs to ensure events are properly logged,
- Performed SSH server command tests,
- Ensured FIPS self-Test is properly functioning,
- Tested 802.1x with OCSP stapling, and
- Performed vulnerability scans of both the entire device and the HTTPS web configuration.

All tests completed satisfactorily.

NIST CAVP Certificates:

The existing CAVP certs were examined and found to still be valid. The underlying FIPS module was unchanged and so no CAVP certification updates were required.

Vulnerability Analysis:

A public search for vulnerabilities that might affect the TOE was performed on 03/24/2022.

The evaluation team performed a search of the following public vulnerability database:

- National Vulnerability Database (https://nvd.nist.gov/).

Searches were performed using the following search terms:

- Crestron
- Crestron DM NVX v5.2 AV-over-IP
- 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-360
- DM-NVX-360C
- DM-NVX-E760
- DM-NVX-E760C
- Intel Arria 10 SX SoC FPGA
- ARM Cortex-A9 MPCore
- lighttpd
- Redis v5.0.5
- openssh
- Net-SNMP
- SafeLogic SSL
- NTPSec
- AV Router
- TLS
- SSH
- HTTPS.

One new vulnerability (CVE-2022-0778) was found using the search string TLS and was fixed in the noted firmware release.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE.

Conclusion:

The overall impact is minor. This is based on the above rationale that new hardware, non-security relevant changes, and the update of the TOE to firmware version 5.2.4651.00032 had no impact on the certified TOE.

In addition, a search for vulnerabilities identified none directly affecting the TOE.

Also, the developer confirmed the changed TOE conforms to NIAP Policy 5, and the existing CAVP certs were found to still be valid.

Therefore, CCEVS agrees that the original assurance is maintained for the product.