ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 10.2

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware and Virtual Appliances all running Panorama 10.2

Maintenance Report Number: CCEVS-VR-VID11285-2023

Date of Activity: 31 May 2023

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, September 12, 2016
- Impact Analysis Report for Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 10.2, Version 1.4, May 30, 2023
- Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 10.2 Security Target, Version 1.0, January 30, 2023
- Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 10.2, Guidance, February 6, 2023
- collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 [NDcPP]

Assurance Continuity Maintenance Report:

Leidos submitted an Impact Analysis Report (IAR) for the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 10.2 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on May 30, 2023. 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 consists of the Security Target (ST), the Administrator's Guide, and the Impact Analysis Report (IAR). The ST and Admin Guide were updated.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Palo Alto Networks Panorama 10.1 Security Target, Version 1.0, June 27, 2022	**Maintained Security Target:** Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 10.2 Security Target, Version 1.0, January 30, 2023 Changes in the maintained ST are: • Document Title - Updated to enumerate specific covered models, consistent with other Palo Alto Networks evaluations • Section 1 – Updated TOE software version and identification of the TOE models • Section 1.1 - Updated identification of ST (title, version, date) • Section 1.1 - Updated TOE software version and models • Section 2.1 - Updated TOE software version and models • Section 2.2.1 – Removed the M-500 hardware appliance; Added the M-300 and M-700 hardware appliances • Section 2.2.1 – Updated the TOE software version and models • Section 2.2.2.2 – Updated the CAVP certificate numbers • Section 2.3 – Identified the most current documentation for the current Panorama release 10.2 Section 6.2 – updated CAVP certificate numbers.
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 10.1, July 22, 2022	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 10.2, February 6, 2023 Changes in the maintained Guidance are: • Updated Document title and revision date • Section 1.2 *TOE References* – Updated

	the version to 10.2.3-h2; added M-300 and M-700 models; removed M-500 model • Section 1.3 *Documentation References* – Updated and identified the current documentation set for the 10.2 release. • Section 7.11 – Updated the TOE version • Section 7.12.7 – Updated the TOE version

Changes to the TOE:

The TOE changes consist of:

- Introduction of the M-300 and M-700 hardware appliances running Panorama 10.2 to the Panorama product line
- Updating the firmware running on the Palo Alto Networks M-200 and M-600 Hardware, and Virtual Appliances from version Panorama 10.1 to version Panorama 10.2. The software updates included new non-security relevant features and bug fixes.
- Palo Alto Networks removed the M-500 hardware appliance from the maintained TOE as it does not support the 10.2 firmware.
- Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for all hardware and virtual appliances, including the new appliances added to the TOE (A2906 for hardware and A2907 for virtual appliances).

Category	Number of Changes	Applicability to New Firmware Versions
New Features and Feature Enhancements	6	The software updates of the PAN-OS 10.1 to PAN-OS 10.2.3 were non-security relevant features and enhancements like Administrator-Level Push, Automatic Content Push for VN-Series and CN-Series Firewalls, and so on.
Bug Fixes	92	92 Bug Fixes were made for issues identified in previous releases of which 2 were security relevant (CVE) Fixes and 90 were behavioral Bug Fixes. The bug-fixes did not result in changes to the ST or guidance documentation and had no effect on the result of any Assurance Activity test.

Regression Testing:

Vendor regression test results were produced and found consistent with the previous test results. Palo Alto performs extensive regression testing for every release including 10.2. Palo Alto conducts automation test suites and performed manual testing.

Equivalency:

The M-300 and M-700 models introduced in this Assurance Continuity activity are considered equivalent to the M-200 and M-600 hardware models in the original evaluated TOE. As described in Section 2.2.1 of the Panorama 10.2 Security Target, the only differences between models are processing power, memory, storage space, and number of network interfaces. This affects the volume of records the TOE can process but does not affect security functionality.

NIST CAVP Certificates:

Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for all hardware and virtual appliances, including the new appliances added to the TOE (A2906 for hardware and A2907 for virtual appliances).

The Palo Alto Networks Crypto Module included with PAN-OS is substantially the same between versions 10.1 and 10.2. The only differences are patches made to address specific published vulnerabilities. The CAVP certificates for v10.2 of the Palo Alto Networks Crypto Module that is included with PAN-OS 10.2 cover the same set of functions and algorithms as obtained for v10.1.

The evaluation evidence presented by Palo Alto Networks for the CAVP certificates from the TOE's original ETR and the evidence for the CAVP certificates for the updated TOE provided equivalence rationale to address any apparent differences between the two sets of certificates.

NIAP reviewed and verified that the CAVP cert changes are not considered major changes and they are the same in the relevant areas to the original certificates. The changes that resulted in the need for new crypto certs do not require a rerun in any of the testing assurance activities.

Vulnerability Analysis:

A new search was performed for vulnerabilities from the time of the original evaluation (27 July 2022) to 30 May 2023. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were detected.

The search was conducted against:

- NIST National Vulnerabilities Database (http://web.nvd.nist.gov)
- US-CERT (http://www.kb.cert.org)
- Palo Alto Networks Security Advisories (https://security.paloaltonetworks.com/).

- "Palo Alto Panorama", "Palo Alto Networks Panorama", and "M-200 Series", "M-500 Series", and "M-600 Series" as variations of the TOE name.
- Processors:
  - Intel Xeon E5-2620
  - Intel Xeon E5-2637
  - Intel Xeon E5-2680
  - Intel Xeon Gold 6248
- Processor microarchitectures:
  - Cascade Lake
  - Ivy Bridge
  - Broadwell
- Software:
  - PAN-OS 10.1

Except as follows:

- "M-300" and "M-700" replace "M-500 Series"
- "Intel Xeon Silver 4310" (processor in M-300) and "Intel Xeon Silver 4316" (processor in M-700) replace "Intel Xeon E5-2637" (processor in M-500)
- "Ice Lake" (microarchitecture for Intel Xeon Silver 4310 and 4316 processors) is added
- "PAN-OS 10.2 replaces "PAN-OS 10.1"

Conclusion:

The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims. The updates described above were made to support the new TOE minor version number.

Regression testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance.

In Addition, Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for all hardware and virtual appliances, including the new appliances added to the TOE (A2906 for hardware and A2907 for virtual appliances).

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