CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.0.4

Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware and Virtual Appliances all running Panorama 11.0.4

Maintenance Report Number: CCEVS-VR-VID11285-2024

Date of Activity: 16 May 2024

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 11.0.4, Version 1.3, May 7, 2024
- Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.0.4 Security Target, Version 1.2, May 7, 2024
- Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 11.0.4, Guidance, May 7, 2024
- 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 11.0.4 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on May 7, 2024. 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 Guides, and the Impact Analysis Report (IAR). The ST and CC Admin Guide were updated.

Documentation updated:

Previous CC Evaluation Evidence	Evidence Change Summary
Security Target: Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.0 Security Target, Version 1.1, September 15, 2023	**Maintained Security Target:** Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.0.4 Security Target, Version 1.2, May 7, 2024 Changes in the maintained ST are: • Document Title - Updated TOE software version • Section 1 - Updated TOE software version • Section 1.1 - Updated identification of ST • Section 1.1 - Updated TOE software version • Section 2.1 - Updated TOE software version Section 2.3 - Updated TOE software version
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 11.0, August 17, 2023	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 11.0.4, May 7, 2024 Changes in the maintained Guidance are: • Document Title - Updated TOE software version and document date • Section 1.2 *TOE References* – Updated the version to 11.0.4 • Section 7.11 *Verify and Update System Software* – Updated TOE software version number • Section 7.12.7 *Structure of REST API Request* – updated sample REST API to reference version 11.0.4
Administrative Guides: • Panorama Administrator Guide, Last Revised: March 13, 2024 • PAN-OS and Panorama API Usage Guide, December 6, 2023 • VM Series Deployment Guide, November 14, 2022	None – no changes made to evaluated hardware and administration guidance is only identified on the 11.0 level because there were no feature enhancements that changed how the product is administered.

Changes to the TOE:

The TOE changes consist of:

- Updating the firmware running on the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances from Panorama 11.02 to Panorama 11.0.4. The software updates included new non-security relevant bug fixes.

Category	Number of Changes	Applicability to New Firmware Versions
Bug Fixes	380	380 Bug Fixes were made for issues identified in previous releases. The 380 bug fixes break out into the following categories: 3 Performance Improvement 57 Behavior Corrections 320 Outside the Scope of the Evaluation Examples of behavior corrections were: Fixed an issue where the managed collectors health status on Panorama displayed as empty, fixed an issue where selective push did not work and fixed an issue on the web interface where the language setting is not retained. None of the bug fixes affected the security functionality and none of the changes resulted in changes to the ST or guidance documentation. These changes were either unrelated to SFR testing or were not visible at the level of testing performed for the SFRs. Thus, the original testing still holds, and any fix testing was covered by vendor non-evaluation regression and checkout testing. CVEs related to PAN-OS affect earlier versions of PAN-OS and do not affect the version on which Panorama 11.0.4 is based or the CVEs are related to other products not the TOE.

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 11.0.4. Palo Alto conducts automation test suites and performed manual testing.

Equivalency:

The security functionality of the Palo Alto Networks M-200, M-300, M-600, and M-700 Hardware, and Virtual Appliances all running Panorama 11.0.4 software update remains the same as the prior evaluated version (running Panorama 10.1) and maintained version (running Panorama 10.2 and 11.0.2). Of particular note, the hardware platforms are unchanged from the previous maintained version.

NIST CAVP Certificates:

The Palo Alto Networks Crypto Module included with Panorama is the same between versions 11.0.2 and 11.0.4, therefore new CAVP certificates were not required.

Vulnerability Analysis:

A new search was performed for public vulnerabilities from the time of the current validated release of the TOE (15 September 2023) to 7 May 2024. 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/).

The search covered the following:

- "Palo Alto Panorama", "Palo Alto Networks Panorama", and "M-200 Series", "M-300 Series", "M-600 Series", and "M-700 Series" as variations of the TOE name.
- Processors:
  - Intel Xeon E5-2620
  - Intel Xeon E5-2680
  - Intel Xeon Silver 4310
  - Intel Xeon Silver 4316
  - Intel Xeon Gold 6248
- Processor microarchitectures:
  - Cascade Lake
  - Ice Lake
  - Ivy Bridge
  - Broadwell
- Software:
  - PAN-OS 11.0

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 to SFR claims. 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, the Palo Alto Networks Crypto Module included with Panorama is the same between versions 11.0.2 and 11.0.4, thus new CAVP certificates were not required. Therefore, CCEVS agrees that the original assurance is maintained for the product.