ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks WF-500 and WF-500-B Wildfire 10.2

Palo Alto Networks WF-500 and WF-500-B Wildfire 10.2

Maintenance Report Number: CCEVS-VR-VID11286-2023

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 WF-500 and WF-500-B Wildfire 10.2, Version 1.4, May 30, 2023
- Palo Alto Networks WF-500 and WF-500-B Wildfire 10.2 Security Target, Version 1.0, February 6, 2023
- Common Criteria Evaluated Configuration Guide (CCECG) for Wildfire 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 WF-500 and WF-500-B Wildfire 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 WF-500 WildFire 10.1 Security Target, Version 1.0, August 1, 2022	**Maintained Security Target:** Palo Alto Networks WF-500 and WF-500-B WildFire 10.2 Security Target, Version 1.0, February 6, 2023 Changes in the maintained ST are: • Updated Document Title and date on cover page • Section 1 – updated TOE identification and firmware version • Section 1.1 – updated ST and TOE identification • Section 2 - updated TOE identification and firmware version • Section 2.2 – updated TOE version • Section 2.2.1 – Added the WF-500-B hardware appliance • Section 2.2.2.2 – Updated CAVP number • Section 2.3 – Updated TOE documentation references • Section 5.2.2 – FCS_SSHS_EXT.1.1 updated to conform exactly to PP • Section 6.2 – updated CAVP certificate numbers.
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.1, August 1, 2022, Version 1.0	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.2, February 6, 2023 Changes in the maintained Guidance are: • Updated Document Title and date on cover page • Section 1 – updated reference to Administrator's Guide • Section 1.2 – Updated the version to 10.2.3-h2; added WF-500-B • Section 1.2, under "Documentation References" – Updated and identified the current documentation set for the 10.2 release.

	• Section 6.2 – updated CAVP certificate numbers.

Changes to the TOE:

The TOE changes consist of:

- Introduction of the WF-500-B hardware appliance running 10.2.3-h2 to the TOE
- Updating the firmware running on the Palo Alto Networks WF-500 hardware appliance from version 10.1.6-h4 to version 10.2.3-h2. The updates included new non-security relevant features and bug fixes. The updates and their effects and relevance are summarized below.
- Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for both the WF-500 and WF-500-B appliances (CAVP A2906).

Category	Number of Changes	Applicability to New Firmware Versions
New Features and Feature Enhancements	1	The software updates of the PAN-OS 10.1 to PAN-OS 10.2.3 were non-security relevant features and enhancements. The addition of the WF-500-B appliance was the only new feature applicable to the Wildfire.
Bug Fixes	27	27 Bug Fixes were applicable to Wildfire of which 2 were security relevant (CVE) Fixes and 25 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 WF-500-B appliance introduced in this Assurance Continuity activity is considered equivalent to the WF-500 appliance in the original evaluated TOE. As described in Section 2.2.1 of the WildFire 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. More specifically, both the WF-500 and the WF-500-B run the same binary executable image. Additionally, Palo Alto Networks has obtained updated cryptographic algorithm certificates covering both hardware appliances included in the updated TOE.

NIST CAVP Certificates:

Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementation for both the WF-500 and WF-500-B appliances (CAVP A2906).

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 (3 August 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/).

and used the same terms as the original evaluation:

- "Palo Alto Wildfire", "Palo Alto Networks Wildfire", and "WF-500 Series" as variations of the TOE name.
- Processors: Intel Xeon E5-2620
- Processor microarchitectures: Sandy Bridge

- Software:
  - Wildfire 10.1
  - PAN-OS 10.1.

Except as follows:

- Added “WF-500-B”
- Added “Intel Xeon Silver 4316” (processor in WF-500-B)
- Added “Ice Lake” (microarchitecture for Intel Xeon Silver 4316 processor)
- Added “Wildfire 10.2” and “PAN-OS 10.2”.

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 both the WF-500 and WF-500-B appliances (CAVP A2906).

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