ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks WF-500 and WF-500-B WildFire 11.0

Palo Alto Networks WF-500 and WF-500-B WildFire 11.0

Maintenance Report Number: CCEVS-VR-VID11286-2023-2

Date of Activity: 18 September 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 11.0, Version 1.0, September 15, 2023
- Palo Alto Networks WF-500 and WF-500-B WildFire 11.0 Security Target, Version 1.0, August 11, 2023
- Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.0, Guidance, August 11, 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 11.0 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on September 15, 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 and WF-500-B WildFire 10.2 Security Target, Version 1.0, February 6, 2023	**Maintained Security Target:** Palo Alto Networks WF-500 and WF-500-B WildFire 10.2 Security Target, Version 1.0, August 11, 2023 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 – Updated TOE software version • Section 2.2 – Updated TOE software version • Section 2.2.1 – Updated TOE software version • Section 2.2.2.2 – Updated CAVP certificate numbers • Section 2.3 – Identified the most current documentation for the current WildFire release 11.0 • Section 6.2 – updated CAVP certificate numbers.
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.2, February 6, 2023	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.0, August 11, 2023 Changes in the maintained Guidance are: • Document Title - Updated TOE software version • Section 1 *Introduction* – Updated the version to 11.0 • Section 1.2 *TOE References* – Updated the version to 11.0.1 • Section 1.3 *Documentation References* – Updated and identified the current documentation set for the 11.0 release.

Changes to the TOE:

The TOE changes consist of:

- Updating the firmware running on the Palo Alto Networks WF-500 and WF-500-B appliances from WildFire 10.2 to WildFire 11.0. The updates included new non-security relevant features and bug fixes. The software updates and their effects and relevance are summarized below.

Category	Number of Changes	Applicability to New Firmware Versions
New Features and Feature Enhancements	4	The software updates of the PAN-OS 10.2 to PAN-OS 11.0 were non-security relevant features and enhancements or features excluded from the evaluated configuration such as: Skip Software Version Upgrade, Intelligent Run-Time Memory Analysis, TLSv1.3 Support for Management Access and Support for OCSP Verification through HTTP Proxy.
Bug Fixes	26	26 Bug Fixes were made for issues identified in previous releases. The 26 bug fixes break out into the following categories: 12 Performance Improvement 8 Behavior Corrections 6 Outside the Scope of the Evaluation 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 WildFire 11.0 is based.

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

Equivalency:

The security functionality of the Palo Alto Networks WildFire WF-500 and WF-500-B running version 11.0 software update remains the same as the prior evaluated version (running WildFire 10.1) and maintained version (running WildFire 10.2). Of particular note, the hardware platforms are unchanged from the previous maintained version.

In addition, Palo Alto Networks has obtained updated cryptographic algorithm certificates covering both appliances included in the updated TOE.

NIST CAVP Certificates:

The Palo Alto Networks Crypto Module included with WildFire is substantially the same between versions 10.2 and 11.0. The only differences are patches made to address specific published vulnerabilities. Palo Alto obtained updated CAVP certifications for WildFire 11.0 covering the updated algorithm implementation for the WildFire appliances (A3453). NIAP reviewed and verified that the CAVP certificates were acceptable, and that equivalence was maintained.

Vulnerability Analysis:

A new search was performed for public vulnerabilities from the time of the previous assurance maintenance activity (30 May 2023) to 15 September 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/).

The search covered the following:

- "Palo Alto Wildfire", "Palo Alto Networks Wildfire", "WF-500", and "WF-500-B" as variations of the TOE name.
- Processors:
  - Intel Xeon E5-2620
  - Intel Xeon Silver 4316
- Processor microarchitectures:
  - Ice Lake
  - Sandy Bridge
- Software:
  - WildFire 11.0
  - 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, Palo Alto Networks obtained updated CAVP certificates covering the updated algorithm implementations for the WildFire appliances, including to support the patches for the processors for the TOE (A3453). Therefore, CCEVS agrees that the original assurance is maintained for the product.