ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks WF-500 and WF-500-B WildFire 11.0.4

Palo Alto Networks WF-500 and WF-500-B WildFire 11.0.4

Maintenance Report Number: CCEVS-VR-VID11286-2024

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 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 11.0.4 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 WF-500 and WF-500-B WildFire 11.0 Security Target, Version 1.0, August 11, 2023	Palo Alto Networks WF-500 and WF-500-B WildFire 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, 2.2, 2.2.1 – Update TOE software version Section 2.3 – Update TOE software version and Guide date
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.0, August 11, 2023	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.0.4, May 7, 2024 Changes in the maintained Guidance are: • Document Title – Updated TOE software version • Section 1.2 *TOE References* – Updated the version to 11.0.4
Administrative Guides: • Palo Alto Networks WildFire Appliance Administrator Guide, Last Revised: August 23, 2023 • WF-500 WildFire Appliance Hardware Reference Guide, February 29, 2016 • WF-500-B WildFire Appliance Hardware Reference Guide, June 6, 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 WF-500 and WF-500-B appliances from WildFire 11.0.2 to WildFire 11.0.4. The updates included bug fixes. The software updates and their effects and relevance are summarized below.

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: 1 Performance Improvement 1 Behavior Correction 378 Outside the Scope of the Evaluation The behavior correction was: "Fixed an issue where the root-cert was set to expire on December 31, 2023. With this fix, the expiration date has been extended." 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 11.0.4 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 WildFire WF-500 and WF-500-B running version 11.0.4 software update remains the same as the prior evaluated version (running WildFire 10.1) and maintained version (running WildFire 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 WildFire 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 last search for vulnerabilities (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 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 the bug fixes 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 WildFire 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.