ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Palo Alto Networks WF-500 with WildFire 9.1.8

Palo Alto Networks WF-500 with WildFire 9.1.8

Maintenance Report Number: CCEVS-VR-VID11081-2021

Date of Activity: 21 April 2021

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Palo Alto Networks WF-500 WildFire with 9.1.8, 16 March 2021
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

Assurance Continuity Maintenance Report:

Leidos submitted an Impact Analysis Report (IAR) for the *Palo Alto Networks WF-500 WildFire with 9.1.8* to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 16 March 2021. 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, the Operational User Guide, PAN-OS Release Notes Version 9.1.8, and the Impact Analysis Report (IAR). The ST and User Guide were both updated. The release notes and IAR were new documents.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes

Security Target: Palo Alto Networks WF-500 WildFire with 9.1.8, Version 1.0, March 16, 2021	Changes in the maintained ST are: • Updated identification of ST • Section 1 *Security Target Introduction* - Updated TOE software version • Section 1.1 *Security Target, TOE and CC Identification* – Updated the TOE version and document dates. • Section 2 *Product Description* - Updated the WildFire software version number • Section 2.2 *TOE Architecture* - Updated the WildFire version number • Section 2.2.1 Physical Boundaries - Updated the WildFire version number • Section 2.3 TOE Documentation – Identified the most current documentation for the current Wildfire release 9.1.8
Guidance: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 9.1.8, Version 1.0, March 16, 2020	Changes in the maintained Guidance are: • Section 1.2 *TOE References* – Updated the version to 9.1.8 • Section 1.3 *Documentation References* – Updated and identified the current documentation set for the 9.1.8 release.

Changes to the TOE:

Palo Alto Networks WF-500 with WildFire 9.1.8 (hereafter WF-500, i.e., the TOE) is a physical appliance composed of the WildFire functional component hosted on the PAN-OS operating system. PAN-OS, an operating system derived from the Linux kernel version 3.10.88, is used in all Palo Alto Networks next-generation firewalls, Panorama, and the WF-500 product lines. It provides different services to each product line.

The change in the TOE version number from 9.0 to 9.1.8 is due to the release of various patch and feature updates that have taken place since the original WF-500 evaluation in 2020. Those changes were exclusively for the PAN-OS portion of the TOE, where WF-500 is formed from the combination of the WildFire component and the underlying PAN-OS operating system. None of those updates involved changes to WildFire component functionality or its security.

The software changes fell into the following categorization:

Major Changes

None.

Minor Changes

The minor changes were collected in two different groups: new features added to PAN-OS, and bug fixes:

- New Features for PAN-OS that are not applicable to the WildFire component and have no impact on the security functionality or the SFRs identified in the WF-500 Security Target, and
- Bug Fixes, also only for PAN-OS, where no changes were made directly to the WildFire component and have no security impact on the WF-500.

New Features

The section "Features Introduced in PAN-OS 9.1" in *PAN-OS Release Notes Version 9.1.8* reports on the new features added to PAN-OS. Those features are all related to services provide for other Palo Alto products and do not directly impact the WF-500.

The new features were introduced for the Palo Alto Networks next-generation firewalls and Panorama products, which run on the same PAN-OS as WF-500 but offer different services. The features do not affect the security claims in the WF-500 Security Target. However, they necessitated the updating the Operating System from version 9.1.0 to 9.1.8 to accommodate the new features.

Bug Fixes

The section "PAN-OS 9.1 Addressed Issues" in *PAN-OS Release Notes Version 9.1.8* contains a list of bug fixes made to PAN-OS. The bug fixes corresponded to patch releases issued since the original WF-500 evaluation. The changes were collected into 11 separate patch releases, all for PAN-OS.

The bug fixes were developed to correct minor problems in all the related Palo Alto products, including the WildFire component.

There were bug fixes for PAN-OS that impacted the WildFire component, but no fixes for the WildFire component itself. The bug fixes related to the WildFire component were determined to be either for features and services not supported in the evaluated configuration (i.e., interactions with firewall or cloud services) or for WildFire interactions with PAN-OS (i.e., incorrect message display, requests causing PAN-OS processing delays).

The new features, and bug fixes, did not change the implementation of any WF-500 SFRs, or result in modifications to WF-500 Security Functions, Assumptions, Objectives, or Assurance Documents. They are all considered to be **minor** changes.

The WF-500 security target and the Common Criteria Evaluation Guidance Document were updated to reflect the operating system version update.

Regression Testing:

The Vendor conducted regression testing and found the results consistent with the previous test results. Palo Alto performed regression testing for every release including 9.1.8. Palo Alto and utilized automated test suites. Manual testing was also performed. All tests produced results as expected and no problems were reported.

NIST CAVP Certificates:

The WF-500 updates did not affect the existing CAVP certificates. The Palo Alto Crypto Module, with the CAVP certificate C1005, has remained unchanged since the previous WF-500 evaluation. The cryptographic primitives have not been affected by the product updates and the C1005 CAVP certificate remains valid for this Assurance Maintenance action.

Vulnerability Analysis:

A public search, for vulnerabilities that might affect the TOE since the original WF-500 evaluation was completed, was performed.

The vulnerability searches were performed on the following Palo Alto product posted on the NIAP Product Compliant List.

- CCEVS-VR-VID11081-2020 - Palo Alto Networks WF-500 with WildFire 9.0. Certificate Date: Certificate Date: 2020.07.20.

The original search terms for the evaluation listed above are provided below. All searches were performed on 3/15/2021and go back to the earliest date of 7/2/2020 to cover all evaluations.

Databases used for the searches:

- http://web.nvd.nist.gov/view/vuln/search
- https://securityadvisories.paloaltonetworks.com

Search Terms:

- Microarchitectural (category of processor vulnerability)
- Xeon (processor type)
- Palo Alto (vendor)
- WildFire (TOE name)
- WF-500 (TOE hardware)
- PAN-OS (TOE software platform)
- Linux 3.10 (OS kernel that PAN-OS is derived from)
- TCP (required by ND-SD)
- SSH (supported protocol)
- TLS (supported protocol)

Summary of the analysis

The vulnerability search found no vulnerabilities that were applicable to the TOE or that were not mitigated or corrected in the TOE via the minor version update.

Conclusion:

The descriptions of all changes were examined and the overall impact considered to be minor. This is based on the above rationale that new features and bug fixes to update the PAN-OS to version 9.1.8 have no Security Relevance on the certified TOE.

In addition, the developer confirmed the changed TOE conforms to NIAP Policy 5. The Palo Alto Crypto Module did not change and CAVP certificate C1005 remains valid. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE.

Therefore, CCEVS agrees that the original assurance is maintained for the WF-500.