ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks WF-500 with WildFire 10.0.5

Palo Alto Networks WF-500 with WildFire 10.0.5

Maintenance Report Number: CCEVS-VR-VID11081-2021

Date of Activity: 17 May 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 10.0.5, IAR v1.1, 18 May 2021
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

Assurance Continuity Maintenance Report:

Leidos submitted *Palo Alto Networks WF-500 WildFire with 10.0.5 Impact Analysis Report* (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 11 May 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 10.0.5, and the IAR. The ST and User Guide were both updated. The release notes and IAR were new documents.

Changes to Evaluation Documentation:

Evidence Identification	Effect on Evidence/ Description of Changes

Security Target: Palo Alto Networks WF-500 with WildFire 9.1.8 Security Target, Version: 1.0, Date: March 16, 2021	**Maintained Security Target:** Palo Alto Networks WF-500 WildFire with 10.0.5 Security Target, Version: 1.1, Date: May 18, 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 10.0.5 • Updated Section 2.4 Excluded Functionality – Updated Table 2 to exclude the IPv6 functionality.
Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 9.1.8, Revision Date: March 16, 2021 Version: 1.0	**Maintained Common Criteria Compliance Guide:** Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.0.5, Revision Date: May 18, 2021, Version: 1.1 Changes in the maintained Guidance are: • Section 1.2 *TOE References* – Updated the version to 10.0.5 • Section 1.3 *Documentation References* – Updated and identified the current documentation set for the 10.0.5 release. • Section 6.4 *Configure SSH Encryption Algorithms (Required)* - SSH profile feature caused the commands to change slightly. • Section 6.5 *Configure SSH Rekey Interval (Required)* - SSH profile feature caused the commands to change slightly. • Section 1.1 *Common Criteria (CC) Evaluated Configuration* – Updated the Scope of Evaluation Table to excluded IPv6 support.

Changes to the TOE:

Palo Alto Networks WF-500 with WildFire 10.0.5 (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 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 9.1.8 to 10.0.5 is due to the release of various patches, and feature updates, that have happened since the WF-500 Assurance Maintenance Action on April 21, 2021. Those changes were for both the PAN-OS portion of WF-500, and WildFire. However, none of those updates involved evaluated WildFire 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 WildFire; and bug fixes:

New Features

The section "Features Introduced in PAN-OS 10.0" in *PAN-OS Release Notes Version 10.0.5* includes updates from the Palo Alto Networks next-generation firewalls, Panorama, and WF-500 product lines.

All new features identified in the Release Notes, that are applicable to the WildFire functional component of WF-500, are identified below. None of them have any impact on the Security Functional Requirements (SFRs) identified in the WF-500 Security Target.

In particular, the new feature for IPv6, addressing support for the WildFire appliance, has not been tested and is out of scope. The ST and AGD have been updated to exclude this functionality.

New WildFire Feature	Description	Impact
WildFire® Inline ML	The firewall is now capable of analyzing Windows executables and PowerShell scripts using machine learning on the dataplane. This enables you to intercept malware before it can infiltrate your network by providing real-time analysis capabilities on the firewall, which reduces the possibility of proliferation of unknown malware variants.	**Minor Change** – This operational functionality of TOE is excluded from the collaborative Protection Profile for Network Devices, Version 2.1. This new feature does not have any impact on the Security Target or the security functionality claimed by the SFRs.
WildFire® Real-Time Signature Updates	WildFire antivirus signatures are now globally distributed in real-time as soon as new verdicts are available. This gives you almost instant access to Palo Alto Networks complete global intelligence data	**Minor Change** - This operational functionality of TOE is excluded from the collaborative Protection Profile for Network Devices, Version 2.1. The distribution of antivirus

New WildFire Feature	Description	Impact
	that is collected from a multitude of enforcement points and that provides additional leverage for preventing successful attacks by minimizing your exposure time to malicious activity, which effectively reduces your infrastructure attack surface and the resulting damage malware can have within your network.	signatures were not included in the evaluation. This new feature does not have any impact on the Security Target or the security functionality claimed by the SFRs.
IPv6 Address Support for the WildFire Appliance	The WildFire appliance now supports IPv6 connections, expanding the number of devices from which it can receive suspicious files and return safety verdicts. As the dwindling number of available IPv4 addresses forces you to introduce more IPv6-addressed devices in to your network, this feature guarantees you are still able to leverage the local file analysis capabilities of the appliance.	**Minor Change** – IPv6 was not included in the previous evaluation. The ST and AGD have been updated to explicitly exclude this functionality from evaluation coverage.
Windows 10 Analysis Environment for the WildFire Appliance	The WildFire appliance can now use the Windows 10 operating system to analyze unknown files. This increases the threat prevention coverage of the appliance by enabling it to detect threats crafted for Windows 10 environments.	**Minor Change** – This operational functionality of TOE is excluded from the collaborative Protection Profile for Network Devices, Version 2.1. The detection of threats for Windows 10 environments was not included in the evaluation. This new feature does not have any impact on the Security Target or the security functionality claimed by the SFRs.
Certificate Management Features		
Master Key Encryption Enhancement	On physical and virtual Palo Alto Networks appliances, you can now configure the Master Key to use the AES-256-GCM encryption algorithm to encrypt data. The AES-256-GCM encryption algorithm increases encryption strength to protect keys better and also includes a built-in integrity check. When you change the encryption level to AES-256-GCM, devices use it instead of the AES-256-CBC encryption algorithm when encrypting keys and other sensitive data.	**Minor Change** – The ST already includes AES-256-GCM in FCS_COP.1.1/DataEncryption. This new feature does not have any impact on the Security Target or the security functionality claimed by the SFRs. AES-256-CBC is still the default.
HSM Enhancements	Newer client driver versions are now supported for SafeNet and	**Minor Change** – The HSM appliances were not claimed in the

New WildFire Feature	Description	Impact
	nCipher Hardware Security Module (HSM) appliances: • SafeNet: You can select from versions 5.4.2 or 7.2. Additionally, you can choose to have your firewall authenticate and establish trust using manually generated certificates. • nCipher nShield Connect: Version 12.40.2 is available (backward compatible up to v11.50 for older appliances)	original evaluation or the prior assurance maintenance. The HSM appliances are not applicable to the WildFire evaluation. The ability to add HSM appliances to the operational environment does not have any impact on the Security Target or the security functionality claimed by the SFRs.
SSH Service Profile	In PAN-OS 9.1 and earlier releases, you could generate a new pair of public and private SSH host keys and change other SSH configuration parameters such as the default host key type from the CLI. In PAN-OS 10.0 and later releases, you must create an SSH service profile (**Device** > **Certificate Management** > **SSH Service Profile**) to customize management and HA SSH configurations. You can configure these profiles from the CLI or the firewall or Panorama web interface.	**Minor Change** – This new feature permits the use of a UI interface. The WildFire evaluation does not include a user interface. This new feature does not have any impact on the Security Target or the security functionality claimed by the SFRs.

Bug Fixes:

The section "PAN-OS 10.0 Addressed Issues" in *PAN-OS Release Notes Version 10.0.5* contains a list of bug fixes made to PAN-OS. The bug fixes corresponded to patch releases since the WF-500 Assurance Maintenance Action on April 21, 2021. The changes were collected into 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 for PAN-OS interactions with WildFire (i.e., attempts to download/view WildFire data, Palo Alto Firewall processing of WildFire data, and cloud access of WildFire data).

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 10.0.5. Palo Alto utilized automated test suites, and 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 April 2021 Assurance Maintenance Action. The cryptographic primitives have not been affected by the product updates and the C1005 CAVP certificate remains valid for the v10.0.5 version.

Vulnerability Analysis:

A public search, for vulnerabilities that might affect the TOE, since the 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 WildFire evaluation are provided below. The date of the previous assurance maintenance vulnerability search was conducted on 3/15/2021. All searches below were performed on 5/7/2021.

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)

The vulnerability search found no vulnerabilities that were applicable to the TOE.

Conclusion:

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

In addition, the vendor confirmed that 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.