™ ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8

Maintenance Update of Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8

Maintenance Report Number: CCEVS-VR-VID11063-2021

Date of Activity: 22 April 2021

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8 Impact Analysis Report, Version 1.2, April 18, 2021

Documentation Updated:

Security Target: Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8 Security Target, Version: 1.0, March 15, 2021

The following updates have been made to the ST:

- Identification of changed TOE versions
- Update of Security Target dates
- Update of references to Changed TOE guidance documentation
- Update of excluded features that are out of scope of the evaluation:
    - SD-WAN
    - Include Username in HTTP Header Insertion Entries
    - East-West Traffic Inspection with VM-Series Firewall on VMWare NSX-T

- SAML Authentication
- Proxy Support for Cortex Data Lake

Guidance Documentation: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Firewalls with PAN-OS 9.1.8, Revision Date: March 15, 2021

The following updates have been made to this guidance document:

- Identification of changed TOE versions
- Update of Guidance Document dates and versions
- Update of excluded features that are out of scope of the evaluation:
  - SD-WAN
  - Include Username in HTTP Header Insertion Entries
  - East-West Traffic Inspection with VM-Series Firewall on VMWare NSX-T
  - SAML Authentication
  - Proxy Support for Cortex Data Lake

In addition, the PAN-OS release notes have been updated to reflect these changes.

Assurance Continuity Maintenance Report:

The Palo Alto Networks PA-220 Series, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 9.1.8 IAR was sent to CCEVS for approval in March 2021. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, and the ST and Guidance Documentation were updated as a result of the changes and the security impact of the changes.

Changes to TOE:

- Software changes to the TOE involve updating PAN-OS from version 9.0.9-h1 to version 9.1.8 to accommodate new features outlined below.
  - Several new software features were added to the underlying product associated with the TOE including features related to SD-WAN, APP-ID, workflows, Panorama, USER-ID, GlobalProtect, Virtualization, Networking.
  - One hardware-related feature, Zero Touch Provisioning (ZTP) was added to the underlying product associated with the TOE. This feature is an SD-WAN functionality.
  - Several changes to the default behavior have been implemented in the TOE, including changes related to URL filtering, REST API, URL category, web interface, GlobalProtect, SD-WAN, SAML Authentication, and firewall memory limit.

All of the above listed features are either performance enhancements, outside the scope of the evaluation, or otherwise not relevant to the security functionality of the evaluated TOE. Overall, it has been determined that the updates have "minor impact" to the evaluation.

- Several bugs were fixed in the update of PAN-OS from version 9.0.9-h1 to version 9.1.8 to resolve issues with features that are not covered in the scope of the evaluation or otherwise not relevant to the security functionality of the evaluated TOE. Overall, it has been determined that the bug fixes have "minor impact" to the evaluation.

Regression Testing:

Vendor regression testing was performed via automation test suites as well as manual testing, and the results were found to be consistent with the previous test results. Updates to the evaluated TOE did not affect the CAVP certificates. An updated vulnerability search was performed on 4/22/2021 using the following databases and search terms:

Databases used for the searches:

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

Search terms:

- Linux 3.10 (TOE implements Linux 3.10.88)
- Microarchitectural
- Palo Alto
- N/A - https://securityadvisories.paloaltonetworks.com
- VM-Series
- PAN-OS
- Router
- Switch
- Firewall
- TCP
- UDP
- IPv4
- IPv6
- SSH
- HTTPS
- TLS
- IPsec
- Cavium

The search did not identify any new potential vulnerability that applies to the changed TOE.

Conclusion:

The specific changes made to the product did not affect the security claims in the TOE, including SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment, and therefore is a minor change. The security target and the Common Criteria

Evaluation Guidance Document are updated to reflect the firmware minor version update.

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found it to be **minor**. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.