ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.1.8

Palo Alto Networks M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.1.8

Maintenance Report Number: CCEVS-VR-VID11070-2021

Date of Activity: 22 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 M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.1.8 Impact Analysis Report, Version 1.1, 19 April 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 M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.1.8 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 19 April 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 (ST), the Operational User Guide, and the Impact Analysis Report (IAR). The ST, User Guide, and the IAR were all updated.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Palo Alto Networks M-100, M200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.0, Version: 1.0, Date: June 26, 2020	**Maintained Security Target:** Palo Alto Networks M-100, M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.1.8 Security Target, Version 1.0 March 16, 2021

	Changes in the maintained ST are: • Section 1.1 - Updated identification of ST • Section 1.1 - Updated TOE software version • Section 2.1 - Updated the Panorama version number • Section 2.2.1 - Updated the Panorama version number • Section 2.3 – Identified the most current documentation for the current Panorama release 9.1.8. • Section 2.4 Updated the evaluation excluded features for the new release 9.1.8 product improvements or features.
Guidance: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 9.0, April 29, 2020	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 9.1.8, March 17, 2021 Changes in the maintained Guidance are: • Updated Section *Scope of Evaluation* - Updated the features that are not evaluated and considered out of scope. • 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. • Section 7.11 *Verify and Update System Software* - Updated the version to 9.1.8.

Changes to the TOE:

The TOE consists of the Panorama M-100, M-200, M-500 and M-600 appliances and virtual appliances all running PAN-OS version 9.1.8 (hereafter Panorama, i.e., the TOE). The vendor made software changes to the PAN-OS that addressed bug fixes and added new features to the software, revising it from the evaluated Panorama version 9.0 to version 9.1.8.

TOE new features:

New features have been identified in the table below. Each table includes the feature name and a description of the feature. The description also explains the impact of the feature on the evaluation and its inclusion or exclusion from the evaluation.

Name	Description
SD-WAN	The PAN-OS software can include a native SD-WAN subscription to provide intelligent and dynamic path selection on

Name	Description
	top of what the PAN-OS security software already delivers. Secure SD-WAN provides the optimal end user experience by leveraging multiple ISP links to ensure application performance and scale capacity. The SD-WAN capability is considered out of scope for the Panorama evaluation. The ST and AGD have been updated to exclude this functionality.
SAML Authentication	SAML Authentication is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP). External authentication is outside the scope of the evaluation. The ST and AGD have been updated to exclude this functionality.
Simplified Application Dependency Workflows	You now have simplified workflows to find and manage application dependencies. You can see and address application dependencies immediately in the Application tab as you create a new Security policy rule or add new applications to an existing rule. Commits provide another checkpoint for dependencies. When a policy rule does not include all application dependencies, you can directly access the associated Security policy rule from the Commit dialog to add the required applications. The simplified application dependency workflow does not impact the security functionality or the SFRs in the Panorama.
Increased System Disk for the Panorama Virtual Appliance	To support larger data sets for large-scale firewall deployments, PAN-OS 9.1 gives you the option to expand the Panorama virtual appliance system disk to 224GB. While the 81GB system disk is still supported, increasing the system disk ensures: Sufficient disk space for dynamic updates when managing large-scale firewall deployments. Expand storage for monitoring and reporting for managed firewall health and SD-WAN monitoring and reporting data at high-scale in Panorama mode. This new feature of expanding the Panorama virtual appliance system disk to 224 GB for v9.1 does not affect any of the SFRs or security functionality in the Panorama 9.1.8 Maintenance Assurance.
Automatic Panorama Connection Recovery	To ensure that you do not commit a configuration change that inadvertently causes the firewall to lose connectivity to Panorama, PAN-OS 9.1 can automatically revert the Panorama and firewall configuration to the previous running configuration. For example, if you perform configuration

Name	Description
	changes to the service routes, and as a result the change blocks traffic from the firewall to Panorama, the firewall's hourly connectivity checks can trigger Automatic Panorama Connection Recovery to revert the configuration back to the last running configuration to restore the connection to Panorama. This recovery ensures that a configuration change won't cause a loss in productivity or require you to physically access the firewall. The Automatic Panorama Connection Recovery was not evaluated. Only the secure TLS connections between the firewalls and Wildfire to the TOE were evaluated. The ST and AGD have been updated to exclude this functionality.
PAN-OS REST API request parameters and error responses	The REST API methods now accept the API key only through a custom HTTP header and no longer as a query parameter. To authenticate your REST API request to the firewall or Panorama, use the custom HTTP header X-PAN-Key: <key> to include the API key in the HTTP header. This change applies only to the REST API; the XML API is unchanged. The REST API methods now implement both rename and move with custom HTTP mappings instead of action query parameters. Examples of the new and previous conventions are below. Rename an address: New convention: POST /restapi/<version>/objects/addresses:rename Replaces: POST /restapi/<version>/objects/addresses?action=rename Move a security policy rule: New convention: POST /restapi/<version>/policies/securityrules:move Replaces: POST /restapi/<version>/policies/securityrules?action=move There is a new error response format for all REST API methods. This new format offers consistent and reliable error reporting that includes both human-readable messages and parsable error codes. The format includes overall request status, product-specific error codes, and details that will give the caller the maximum amount of data available if an error does occur.

Name	Description
	The REST API URIs now denote version with a v prefix for versions 9.1 and beyond. Examples of the new and previous conventions are below: New convention: GET /restapi/v9.1/objects/addresses Replaces: GET /restapi/9.0/objects/addresses This change in default behavior does not affect any of the SFRs or security functionality in the Panorama 9.1.8 Maintenance Assurance. No updates are required for the ST or AGD documents.

TOE 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 Panorama evaluation.

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

The bug fixes related to the Panorama 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 Panorama 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 Panorama SFRs, or result in modifications to Panorama Security Functions, Assumptions, Objectives, or Assurance Documents. They are all considered to be **minor** changes.

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

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 9.1.8. Palo Alto conducted automation test suites and performed manual testing.

NIST CAVP Certificates:

The product updates do not affect the CAVP certificates. The Palo Alto Crypto Module with the CAVP certificate C1005 has remained unchanged since the previous v9.0 evaluation. The cryptographic primitives have not been affected by the product updates and the C1005 CAVP certificate remains valid for the v9.1.8 evaluation.

Vulnerability Analysis:

An updated search for vulnerabilities was performed, on the updated TOE, April 19, 2021. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were detected.

Databases used for the searches:

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

The following search terms were used in the updated vulnerability analysis:

- Palo Alto
- Panorama
- PAN-OS
- Management Appliance
- TCP
- SSH
- HTTPS
- TLS
- Microarchitectural
- Linux 3.10

Conclusion:

The overall impact is minor. This is based on the above rationale that updates to Panorama 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 operational environment under which the validated cryptographic algorithm implementation was tested is the same as the operational environment as the changed TOE. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE.

The CCTL also reported that there were no new TOE vulnerabilities. Therefore, CCEVS agrees that the original assurance is maintained for the product.