ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Palo Alto Networks M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 10.0.5

Palo Alto Networks M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 10.0.5

Maintenance Report Number: CCEVS-VR-VID11070-2021-2

Date of Activity: 14 July 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-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 10.0.5 Impact Analysis Report, Version 1.0, 21 June 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-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 10.0.5 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 24 June 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 M100, M200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 9.1.8, Version: 1.0, Date: April 19, 2020	**Maintained Security Target:** Palo Alto Networks M-200, M-500, and M-600 Hardware, and Virtual Appliances all running Panorama 10.0.5 Security Target, Version 1.0 June 21, 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 – Removed the Panorama version number • Section 2.3 – Identified the most current documentation for the current Panorama release 10.0.5. • Section 2.4 Updated the evaluation excluded features for the new release 10.0.5 product improvements or features.
Guidance: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 9.1.8, March 17, 2020	**Maintained Common Criteria Compliance Guide:** Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Panorama 10.0.5, June 21, 2021 Changes in the maintained Guidance are: • Section 1.1 *Common Criteria (CC) Evaluated Configuration* – Updated the Scope of Evaluation to exclude the Scheduled Report functionality • 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 4 *Required Auditable Events* – Updated GUI command screenshots. • Section 5 *Identification and Authentication* - Updated GUI command screenshots. • Section 6 *Evaluated Configuration* - Updated GUI command screenshots and CLI commands • Section 7 *Management Activity* - Updated GUI command screenshots.

Changes to the TOE:

The TOE consists of the Panorama M-200, M-500 and M-600 appliances and virtual appliances all running PAN-OS version 10.0.5 (hereafter Panorama, i.e., the TOE). The Palo Alto Networks M-100 hardware appliance has reached end of life and has been removed from the assurance maintenance. The vendor also has 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 9.1.8 to version 10.0.5.

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
Enhanced Authentication for Dedicated Log Collectors and WildFire Appliances	Dedicated Log Collectors and WildFire appliances now support multiple local admins with granular authentication parameters, as well as remote authentication and authorization leveraging LDAP, RADIUS, or TACACS+ to enable central user management and ensure audit compliance. You can create and manage Log Collector and WildFire admins from the Panorama management server. This new feature is out of scope on the Panorama. The new feature does not change the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Automatic Content Updates Through Offline Panorama	You can now automate content updates for firewalls in an air-gapped network (where Panorama and the firewall are not connected to the internet) to reduce the operational burden and maintain an up-to-date security posture. Now, you can deploy a Panorama server to automatically download content updates from the Palo Alto Networks Update server and export them to an SCP server. On a configured schedule, the air-gapped Panorama retrieves the packages from the SCP server to install on firewalls. The new feature does not change the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Increased Configuration Size for Panorama	The Panorama management server now supports increased configuration size for the M-Series and Panorama virtual appliances without performance impact to tasks such as configuration changes, commits, and pushes to managed firewalls. The new feature does not change the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Syslog Forwarding Using Ethernet Interfaces	Forwarding logs over the management interface can result in loss of logs and impact performance of management tasks due to insufficient bandwidth. Now, you can forward all PAN-OS logs to an external syslog server over an Ethernet interface on the Panorama management server and Dedicated Log Collector. This is not applicable as these are PAN-OS logs (firewall traffic logs) that are sent (i.e., forwarded) to another Panorama configured as a Log Collector. This does not affect the local logs on the Panorama that are sent over TLS to an audit server. The new feature does not change the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Access Domain Enhancements for Multi-Tenancy	IT administrators managing multiple unrelated tenants from a single Panorama can now create Device Group and Template (DG&T) admins with better visibility and control of managed firewalls in their access domains. DG&T admins in multi-tenant environments can now perform essential day-to-day tasks related to firewall management in their access domain. The new feature does not change

Name	Description
	the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Log Query Debugging	You can now view log collector queries to monitor bottlenecks in your deployment. If your log collectors are experiencing impacted performance, you can query all jobs or a specific job ID to better understand why your log query is experiencing issues. The new feature does not change the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Configurable Key Limits in Scheduled Reports	To improve the accuracy of scheduled reports, you can now configure the minimum and maximum key limits Panorama utilizes to generate reports. By increasing the number of keys, Panorama can aggregate, sort, and group larger sets of data to generate more accurate report results. Reports can be configured to run immediately or schedule them to run at specific intervals. The TOE can save and export the reports or email them to specific recipients. The Scheduled Reports capability has not been tested and is considered out of scope for the Panorama evaluation. The ST and AGD have been updated to exclude this functionality. This new feature does not have any effect on the testing or AAR.
Scheduled Reports for Cortex Data Lake	(PAN-OS 10.0.2 or later and Cloud Services plugin 1.8.0 or later) For better visibility into your Cortex Data Lake data, you can now generate scheduled reports on it. NIAP TD0407 excludes the evaluation of cloud deployments and services. The ST and AGD have been updated to exclude this functionality. This new feature does not have any effect on the testing or AAR.

TOE Bug fixes:

The section "*PAN-OS 10.0.5 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 issued since the PAN-OS 9.1.8 assurance maintenance.

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 10.0.5. 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 v10.0.5 evaluation.

Vulnerability Analysis:

An updated search for vulnerabilities was performed, on the updated TOE, June 21, 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 10.0.5 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.