ASSURANCE CONTINUITY MAINTENANCE REPORT FOR PALO ALTO NETWORKS PA-400 SERIES, PA-800 SERIES, PA-1400 SERIES, PA-3200 SERIES, PA-3400 SERIES, PA-5200 SERIES, PA-5400 SERIES, PA-5450, PA-7000 SERIES, AND VM SERIES NEXT-GENERATION FIREWALL WITH PAN-OS 11.2

Maintenance Update of Palo Alto PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.2

Maintenance Report Number: CCEVS-VR-VID11482-2026

Date of Activity: 06 Jul 2026

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 PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.2;

Palo Alto Networks Impact Analysis Report, Version 1.0, June 30, 2026;

Documentation Updated: The original documentation has been updated to the following:

Security Target: Palo Alto Networks PA-400 Series, PA-800 Series, PA-1400 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series, and VM Series Next-Generation Firewall with PAN-OS 11.2 Security Target, Version 1.0, July 8, 2024. Changes in the Security Target are:

- Updated document title on cover page and in page headers
- Updated TOE version number throughout document
- Section 1 – added "PA-455-5G" to list of devices included in TOE
- Section 1.1 – updated ST and TOE identification; added "PA-455-5G" to list of devices included in TOE; removed Ubuntu 18.04 LTS and Microsoft Hyper-V Server 2016 from supported hypervisors for VM-Series
- Section 2.1 – added "PA-455-5G" to list of devices included in TOE
- Section 2.2.1 – added details about PA-455-5G device
- Section 2.3 – Updated TOE documentation references.

Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for Next-Generation Firewalls with PAN-OS 11.2, Revision

Date: July 9, 2024. Changes in the CCECG are:

- Updated TOE version on cover page and page footers
- Section 1.2 – updated TOE version; added PA-455-5G to physical devices in TOE
- Section 1.3 – updated TOE documentation references

Admin Guide: Changes were made to the PAN-OS® Administrator's Guide, Revision Date: April 1, 2026, including:

- TOE version removed from cover page and page footers
- Section "Getting Started" removed
- Section "Firewall Administration" – merged some subsections and reordered some information; added subsection "Configure Response Pages"; removed subsections "Configure 5G for a Cellular Interface" and "Upgrade 5G Firmware"
- Section "Device Telemetry" – deleted subsection "Disable Device Telemetry", which was redundant
- Added section "Security Settings", which is applicable only to PAN-OS 12.1.2 and later
- Section "Authentication" – added subsection "Pre-Logon for SAML Authentication", which provides guidance related to the GlobalProtect app
- Section "Certificate Management" – added background on keys and digital certificates and rearranged guidance related to certificates and certificate revocation
- Section "High Availability" – merged some sections
- Added section "NGFW Clustering"
- Section "App-ID" – rearranged some information
- Removed section "Device-ID"
- Removed section "Decryption" – information merged into "Firewall Administration" section
- Removed section "Quality of Service"– information merged into other sections
- Removed section "Policy" – information merged into other sections
- Section "Virtual System" – re-organized and merged some subsections

Admin Guide: PAN-OS Web Interface Help 11.2, Revision Date: August 8, 2025. Changes in the Admin Guide are:

- Updated TOE version on cover page and page footers
- Page 2 – updated "Last Revised" date
- Section "Objects" – added subsections "Objects > Custom Objects > SaaS Tenant List", "Objects > Custom Objects > SaaS User List", "Objects > Security Profiles > AI Security"
- Section "Network" – added subsection "Network > Traffic Objects"

- Section "Panorama web Interface" – removed subsection "Create and Edit a Firewall Cluster"

Admin Guide: VM-Series Deployment Guide, Version 11.1, Revision Date August 20, 2025. Changes in the Admin Guide are:

- Updated TOE version on cover page and page footers
- Section "About the VM-Series Firewall" – added subsection "Additional XFF IP Logging"
- Section "Set Up the VM-Series Firewall on an ESXi Server" – added subsection "ESXi Simplified Onboarding"
- Section "Set Up the VM-Series Firewall on AWS" – added subsections "VM-Series Integration with AWS Warm Pool", "Simplified Onboarding of VM-Series Firewall on AWS", "AWS Shared VPC Monitoring"
- Section "Set Up the VM-Series Firewall on Azure" – added subsections "Simplified Onboarding of VM-Series Firewall on Azure", "Azure Health Monitoring"
- Section "Set Up the VM-Series Firewall on Google Cloud Platform" – added subsections "Deployment Models for VM-Series on GCP", "Securing VPC Networks with VM-Series Firewall on GCP", "Secure Boot Support for VM-Series on GCP", "Configuring GCP Load Balancer"
- Section "Set Up the VM-Series Firewall on IBM Cloud" – removed subsections "High Resiliency for VM-Series Firewall on IBM Cloud", "Use Case: Deploy a NLB Using the VM-Series Firewall"
- Section "Set Up the VM-Series Firewall on Alibaba Cloud" – added subsection "VM-Series Integration with an Alibaba Gateway Load Balancer"
- Added section "Set up the VM-Series Firewall on Tencent Cloud China"
- Removed section "Endpoint Monitoring for Cisco TrustSec"
- Section "Bootstrap the VM-Series Firewall" – added subsection "Bootstrapping VM-Series in Virtual Metadata Collector Mode"

Admin Guide: PAN-OS® and Panorama™API Usage Guide, Version 11.1 & later, August 21, 2024. Changes in the Admin Guide are:

- Updated TOE version on cover page and page footers
- Page 2 – updated "Last Revised" date

Admin Guide: PAN-OS CLI Quick Start, Version 11.1 & later, May 1, 2024. Changes in the Admin Guide are:

- Updated TOE version on cover page and page footers
- Page 2 – updated "Last Revised" date

- Section "Get Started with the CLI" – merged some subsections and reordered some information.
- Section "Use the CLI" – merged some subsections and reordered some information
- Added new section "CLI Cheat Sheet: CTD Evasion Detection"
- Added new section "CLI Cheat Sheet: Content-ID"
- Section "CLI Changes in PAN-OS 11.1" renamed "CLI Changes in PAN-OS 11.1+" and adds subsections for CLI changes (commands introduced, changed, and removed) in PAN-OS 11.2 and PAN-OS 12.1.
- Section "CLI Command Hierarchy for PAN-OS 11.1" renamed "CLI Command Hierarchy for PAN-OS 11.1+" and adds subsections for PAN-OS 11.2 CLI Ops command hierarchy and Configure CLI command hierarchy.

TOE software:

- Updated from PAN-OS version 11.1.4 to version 11.2.10-h9
- Removal of Ubuntu 18.04 LTS and Microsoft Hyper-V Server 2016 from the supported hypervisors for the VM-Series firewalls

TOE Hardware:

- Addition of the **PA-455-5G** (equivalent to the PA-450R and PA-450-5G).

Assurance Continuity Maintenance Report:

Palo Alto Networks, Inc. submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the CCEVS for approval in April 2026. The IAR is intended to satisfy the 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 validated TOE, the evidence updated because of the changes, and the security impact of the changes.

Changes to TOE consist of introduction of a new hardware appliance, software updates adding features that do not affect the evaluated security functionality, software corrections, and bug fixes. An updated public vulnerability search was performed on June 30, 2026, and all potential vulnerabilities were determined to be mitigated/fixed or not applicable to the evaluated configuration. No residual vulnerabilities were identified.

Changes to TOE:

Palo Alto Networks, Inc. updated the TOE PAN-OS from the evaluated version11.1.4 to version 11.2.10-h9 (Table 1), adding new features, and introducing a new hardware appliance, the PA-455-5G. The feature additions did not affect the security claims in the PAN-OS Security Target, and there were no changes to SFRs, Security Functions, Assumptions, or Objectives, Assurance Documents, or TOE Environment. Vendor regression testing, comprising execution of automation test suites and additional manual testing, produced test results consistent with the previous test results.

Hardware Changes

An additional TOE hardware model/variant of the product was added, the PA-455-5G firewall for industrial, commercial, government, and enterprise deployments that rely on cellular activity. The PA-455-5G is equivalent to the PA-450R and PA-450-5G having the same number and type of ports (eight RJ-45 10/100/100 Ethernet, one RJ-45 for GUI access, one RJ-45 serial console, two USB, one micro-USB, and Power), and processor (Intel Atom C3708).

NIST CAVP Certificates

The new hardware variant **does not** impact the CAVP Certificate – the same certificate (A3453) from the evaluated TOE applies to the PA-455-5G. The CAVP certificate to SFR mappings in Table 8 of the ST are unchanged and remain valid in the TOE using PAN-OS version 11.2.

The impact of the additional hardware variant is considered **minor**.

Software Changes

Software changes consist of updates to Palo Alto Networks PAN-OS from version 11.1.4 to version 11.2.10-h9. The updates comprise:

- Forty-four (44) new non-security relevant features and enhancements
- Bug fixes.

Table 1 – Non-Security Relevant Features Introduced in PAN-OS Version 11.2

Features Added to PAN-OS Versions 11.2	
Feature	**Impact Analysis**
Regional Service Domain Control for Advanced DNS Security	**Minor**: This feature improves usability without affecting evaluated security functionality.
Support For Brotli Decompression	**Minor**: This feature adds capability without affecting evaluated security functionality.
Advanced DNS Security	**Minor**: This feature improves usability without affecting evaluated security functionality.
Local Deep Learning for Advanced Threat Prevention	**Minor**: This feature improves usability without affecting evaluated security functionality.

Features Added to PAN-OS Versions 11.2	
Feature	**Impact Analysis**
Accelerate Insights and Enhance Security with Telemetry Auto-enablement	**Minor**: This feature improves usability without affecting evaluated security functionality.
Configuration File Compression	**Minor:** This feature improves the performance of communications between Panorama and the TOE without affecting evaluated security functionality.
Strata Cloud Manager Connectivity Using Port 443	**Minor**: Management using Strata Cloud Manager is excluded from the evaluated configuration.
View Preferred and Base Releases of PAN-OS Software	**Minor**: This feature applies to Panorama and not to the TOE.
Support for HTTP/2 Networking	**Minor:** HTTP is disabled by default and cannot be enabled in the evaluated configuration.
Preventing DoS Attacks with Enhanced DoS and PBP Configurations	**Minor**: This feature improves usability without affecting evaluated security functionality.
IPv6 Support on Cellular Interface for PA-415-5G Firewall	**Minor**: This feature improves usability without affecting evaluated security functionality.
Encrypted DNS for DNS Proxy and the Management Interface	**Minor**: This feature adds capability without affecting evaluated security functionality.
Post Quantum Hybrid Key Exchange VPN	**Minor:** The use of Post-Quantum Hybrid Key Exchange is excluded from the evaluated configuration.
Increased Maximum Number of Security Rules for the PA-3400 Series Firewall	**Minor**: This feature adds capability without affecting evaluated security functionality.

Features Added to PAN-OS Versions 11.2	
Feature	**Impact Analysis**
Authenticate LSVPN Satellite with Serial Number and IP Method	**Minor:** LSVPN Satellite authentication with Serial Number and IP is excluded from the evaluated configuration.
Secure Custom AI Models on Private Endpoints	**Minor**: This feature applies to Panorama and not to the TOE.
Panorama AI Security Log Enhancements	**Minor**: This feature applies to Panorama and not to the TOE
Prisma AIRS AI Runtime Support in Panorama	**Minor**: This feature applies to Panorama and not to the TOE.
Zero Touch Provisioning (ZTP) Onboarding Enhancements	**Minor**: This feature applies to Panorama and not to the TOE.
GTP Support for Intelligent Security	**Minor:** GTP Support for Intelligent Security is excluded from the evaluated configuration.
TLSv1.3 Support for HSM Integration with SSL Inbound Inspection	**Minor:** SSL Inbound Inspection is excluded from the evaluated configuration.
User Session Tracking for SaaS Security Inline	**Minor:** SaaS Security Inline subscription service is excluded from the evaluated configuration.
Additional HTTP Header Logging for More Tenant-Level Detection	**Minor:** SaaS Security Inline subscription service is excluded from the evaluated configuration.
Explicit Proxy Support for Advanced Services	**Minor:** Advanced cloud subscription services are excluded from the evaluated configuration.
Post-Quantum IKEv2 VPNs Support	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.
Add SD-WAN Capability to your Cellular Interfaces (4G/5G)	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.

Features Added to PAN-OS Versions 11.2	
Feature	**Impact Analysis**
Multiple Virtual Routers Support on SD-WAN Branches	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.
Monitor Bandwidth on SD-WAN Devices	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.
Multiple Virtual Routers Support on SD-WAN Hubs	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.
Additional Private Link Types Support on SD-WAN Device	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.
Additional SD-WAN Hubs in VPN Cluster	**Minor:** SD-WAN subscription service is excluded from the evaluated configuration.
Additional XFF logging for VM-Series firewall in GCP	**Minor:** VM subscription service is excluded from the evaluated configuration.
Bootstrapping VM-Series in Virtual Metadata Collector Mode	**Minor:** VM subscription service is excluded from the evaluated configuration.
Intelligent Traffic Offload - NAT Support on VM-Series Firewall	**Minor:** VM subscription service is excluded from the evaluated configuration.
Intelligent Traffic Offload - L3 (Dynamic Routing) Support on VM-Series Firewall	**Minor:** VM subscription service is excluded from the evaluated configuration.
Intelligent Traffic Offload - Support for NVIDIA Bluefield-3 DPU	**Minor:** VM subscription service is excluded from the evaluated configuration.
Virtual Systems Support on VM-Series Firewall	**Minor:** VM subscription service is excluded from the evaluated configuration.

Features Added to PAN-OS Versions 11.2	
Feature	**Impact Analysis**
Advanced Threat Prevention (ATP) Support on CN-Series Firewall	**Minor:** CN-Series firewall is excluded from the evaluated configuration.
User-ID for CN-Series	**Minor:** CN-Series firewall is excluded from the evaluated configuration.
GlobalProtect Support for PAN-OS-11.2-DHCP-Based IP Address Assignments	**Minor**: This feature improves usability without affecting evaluated security functionality.
CIE (SAML) Authentication using Embedded Web-view	**Minor:** SAML authentication of GlobalProtect users is excluded from the evaluated configuration.
SAML Authentication for GlobalProtect Portals on Non-Standard Ports	**Minor:** SAML authentication of GlobalProtect users is excluded from the evaluated configuration.
PA-455-5G Next-Generation Firewall	**Minor:** The PA-455-5G firewall is considered equivalent to the PA-450R and PA-450R-5G already included in the TOE.
Automatic Certificate Renewal for Passive HA Devices	**Minor**: This feature improves usability without affecting evaluated security functionality.

Addressed Issues:

In addition to the new features enumerated in Table 1, Palo Alto Networks addressed sixteen hundred and two (1,602) issues in PAN-OS releases 11.2. None of the changes addressing these issues resulted in changes to the ST or guidance documentation, and had no effect on security functionality or the result of any Assurance Activity test. These issues are summarized for each version release in Table 2 from the full list available in the IAR.

Table 2 – Issues Addressed in PAN-OS 11.2

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.0	Twenty-Six (26) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS.
11.2.0-H1	One (1) Issue Addressed	**Minor Changes** – Hot-fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474, improving security posture without affecting security functionality.
11.2.1	Nine (9) Issues Addressed	**Minor Change**s – Improved usability, reliability, or corrected product behavior without affecting security functionality, or applied only to Panorama, not PAN-OS, or VM Series Firewalls which were excluded from the evaluated configuration.
11.2.1-H1	One (1) Issue Addressed	**Minor Changes** – Hot-fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474, improving security posture without affecting security functionality.
11.2.2	Six (6) Issues Addressed	**Minor Change**s – Improved reliability without affecting security functionality, or applied only to VM Series Firewalls or the use of decryption policies, which were excluded from the evaluated configuration; or applied only to the WildFire WF-500 appliances, which are not in the TOE.
11.2.2-H1	One (1) Issue Addressed	**Minor Change** – Improved usability without affecting security functionality.
11.2.2-H2	One (1) Issue Addressed	**Minor Changes** – Hot-fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474, improving security posture without affecting security functionality.

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.3	One Hundred and Twenty-Seven (127) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies, which are excluded from the evaluated configuration; or applied to VM Series Firewalls on Microsoft Azure Environments, CN Series Firewalls, or PA 220 Firewalls not included in the TOE.
11.2.3-H1	Hot-fix not made available	N/A
11.2.3-H2	Hot-fix not made available	N/A
11.2.3-H3	Three (3) Issues Addressed	**Minor Changes** – Improved usability without affecting security functionality; and hot-fix made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474, improving security posture without affecting security functionality.
11.2.3-H4	Hot-fix not made available	N/A
11.2.3-H5	Six (6) Issues Addressed	**Minor Changes** – Improved usability, reliability, or performance without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to Cloud NGFW, which is not included in the TOE.
11.2.4	Thirty-Seven (37) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to Cloud NGFW, which is not included in the TOE.
11.2.4-H1	Eight (8) Issues Addressed	**Minor Changes** – Hot-fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474, improving security posture without affecting security functionality.

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.4-H2	Four (4) Issues Addressed	**Minor Changes** – Improved usability, reliability, or performance without affecting security functionality; or applied only to the WildFire WF-500 appliances, which are not in the TOE.
11.2.4-H3	Hot-fix not made available	N/A
11.2.4-H4	Twenty-Three (23) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies, which are excluded from the evaluated configuration; or applied to Panorama M-300 and WildFire WF-500 appliances, which are not in the TOE; or hot-fixes made to address CVE-2025-0111, CVE-2025-0108, and CVE-2025-0109, improving security posture without affecting security functionality.
11.2.4-H5	Seven (7) Issues Addressed	**Minor Changes** – Improved reliability or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to Panorama appliances, which are not in the TOE
11.2.4-H6	Eighteen (18) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS.

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.4-H7	Seven (7) Issues Addressed	**Minor Changes** – Improved usability or reliability without affecting security functionality; or applied to a configuration that is not included in the TOE.
11.2.4-H8	Two (2) Issues Addressed	**Minor Changes** – Improved reliability without affecting security functionality;
11.2.4-H9	Thirty-Eight (38) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to configurations, which are not in the TOE; or a hot-fix made to address CVE-2025-0133, improving security posture without affecting security functionality.
11.2.4-H10	Forty-Seven (47) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies excluded from the evaluated configuration; or applied to Panorama Appliances, which are not in the TOE.
11.2.4-H11	Ten (10) Issues Addressed	**Minor Changes** – Improved reliability or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies excluded from the evaluated configuration; or applied to configurations, which are not in the TOE.
11.2.4-H12	Twenty-Eight (28) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies excluded from the evaluated configuration; or applied to Panorama Appliances or configurations, which are not in the TOE.
11.2.4-H13	Hot-fix not made available	N/A

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.4-H14	Twenty-Seven (27) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS.
11.2.4-H15	One (1) Issue Addressed	**Minor Change** – Hot-fix was made to address CVE-2026-0227, improving security posture without affecting security functionality.
11.2.5	Two Hundred and Three (203) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to external authentication servers that would use PEAP-MSCHAPv2 authentication, which is excluded from the evaluated configuration; or applied to a Configuration or PA-220 firewalls, which are not in the TOE.
11.2.5-H1	One (1) Issue Addressed	**Minor Changes** – Applied only to Panorama AI Runtime Security, not PAN-OS.
11.2.5-H2	One (1) Issue Addressed	Applied to Panorama M-600 and M-700 appliances, which are not in the TOE.
11.2.6	Seventy-Eight (78) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies, which are excluded from the evaluated configuration; or applied to a Configuration or Panorama M-600 and M-700 appliances, which are not in the TOE.

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.7	One Hundred and Forty-Three (143) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of Kerberos Authentication or decryption policies, which are excluded from the evaluated configuration; or applied to Configurations, DNS Security subscriptions, App-ID Cloud Engine subscriptions, PA-220 firewalls, or WildFire and Panorama appliances, which are not in the TOE.
11.2.7-H1	Nineteen (19) Issues	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of decryption policies, which are excluded from the evaluated configuration.
11.2.7-H2	Seven (7) Issues	**Minor Changes** – Improved reliability or corrected product behavior without affecting security functionality; or applied to Configurations, which are not in the TOE.
11.2.7-H3	Twenty-One (21) Issues Addressed	**Minor Changes** – Improved usability or reliability without affecting security functionality; or applied only to Panorama, not PAN-OS.
11.2.7-H4	Forty-One (41) Issues Addressed	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to SSL Decryption and Decryption Policies, or Strat Cloud Firewall Manager, which are excluded from the evaluated configuration; or applied to Prisma Access orWildFire, which are not in the TOE.
11.2.7-H5	Hot-fix not made available	N/A
11.2.7-H6	Hot-fix not made available	N/A

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.7-H7	Three (3) Issues Addressed	**Minor Changes** – Improved reliability without affecting security functionality.
11.2.7-H8	Thirty-Three (33) Issues Addressed	**Minor Changes** – Improved capacity, usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS.
11.2.7-H9	Hot-fix not made available	N/A
11.2.7-H10	Sixteen (16) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of TLS and SSL decryption policies, which are excluded from the evaluated configuration; or applied to configurations or Prisma Access, which are not in the TOE.
11.2.8	Three Hundred and Ninety-Two (392) Issues Addressed	**Minor Changes** – Improved capability, capacity, usability, reliability, performance, problem determination, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of the Strata Cloud Manager and Logging Service, TLS Decryption policies, SSL Decryption, or Decryption Policies, which are excluded from the evaluated configuration; or applied to the console or HTTP which are disabled in the evaluated configuration; or applied to Configurations, VM-Series on Microsoft Azure, or WildFire, which are not in the TOE; or hot-fixes made to address possible security vulnerabilities, improving security posture without affecting security functionality.
11.2.9	Fourteen (14) Issues Addressed	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied only to Panorama, or applied to Prisma Access or WildFire, which are not in the TOE.

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.10	Sixty-Seven (67) Issues Addressed	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of Strata Cloud Manager and Logging Service, or SSL decryption policies, which are excluded from the evaluated configuration; or applied to Configurations, Prisma Access, WildFire, or Panorama Appliances, which are not in the TOE.
11.2.10-H1	Four (4) Issues Addressed	**Minor Changes** – Improved reliability without affecting security functionality.
11.2.10-H2	Twenty (20) Issues Addressed	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to Configurations, which are not in the TOE.
11.2.10-H3	Ten (10) Issues Addressed	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to Configurations, which are not in the TOE.
11.2.10-H4	Twelve (12) Issues Addressed	**Minor Changes** – Improved usability, reliability, or corrected product behavior without affecting security functionality; or applied to TLS and SSL decryption policies, which are excluded from the evaluated configuration.
11.2.10-H5	Thirty-three (33) Issues Addressed	**Minor Changes** – Improved usability, reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to Configurations, which are not in the TOE.
11.2.10-H6	Ten (10) Issues Addressed	**Minor Changes** – Improved reliability, performance, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or hot-fixes made to address possible security vulnerabilities, improving security posture without affecting security functionality.

ISSUES ADDRESSED IN PAN-OS 11.2		
PAN-OS Version	**Number of Addressed Issues**	**Analysis**
11.2.10-H7	One (1) Issue Addressed	**Minor Change** – Hot-fix was made to address CVE-2026-0257, improving security posture without affecting security functionality.
11.2.10-H8	Two (2) Issues Addressed	**Minor Changes** – Improved reliability without affecting security functionality.
11.2.10-H9	Two (2) Issues Addressed	**Minor Changes** – Improved reliability without affecting security functionality; or hot-fixes made to address possible security vulnerabilities, improving security posture without affecting security functionality.

Vulnerability Searches:

The evaluation team for Palo Alto Networks PAN-OS 11.1 performed a final search for vulnerabilities in the TOE on 17-Sep-2024 in the following public vulnerability repositories:

- National Vulnerabilities Database (NVD) (https://nvd.nist.gov/vuln/search)
- US-Cert (https://www.kb.cert.org/vuls/)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- Palo Alto Networks Security Advisories (https://security.paloaltonetworks.com/).

Table 3 – Search Terms Used in the Vulnerability Database Search

SEARCH TERMS	
Search Class	**Search Terms**
Processors	"AMD EPYC 7352", "AMD EPYC 7452", "AMD EPYC 7642", "AMD EPYC 7742", "AMD EPYC 7003", "Cavium Octeon CN7130", "Cavium Octeon CN7240", "Cavium Octeon CN7350", "Cavium Octeon CN7360", "Cavium Octeon CN7885", "Cavium Octeon CN7890", "Intel Atom C3436L", "Intel Atom C3558R", "Intel Atom C3708", "Intel Atom C3758R", "Intel Atom C5325", "Intel Atom C5335C1", "Intel Atom P5332", "Intel Atom P5342", "Intel Atom P5352", "Intel Atom P5362", "Intel Atom P5752", "Intel Pentium D1517", "Intel Xeon D1548", "Intel Xeon D1567", "Intel Xeon D-2187NT", "Intel D-2798NX", "Intel Xeon Gold 6248"

SEARCH TERMS	
Search Class	**Search Terms**
Microarchitectures	"MIPS64", "Zen 2", "Zen 3", "Denverton", "Tremont", "Skylake", "Ice Lake", "Broadwell"
Software	"PAN-OS 11.1", "NGINX 1.20.1"
Variations of the TOE Name	"Palo Alto Firewall", "Palo Alto Networks Firewall", and "PA-400 Series", "PA-800 Series", "PA-1400 Series", "PA-3200 Series", "PA-3400 Series", "PA-5200 Series", "PA-5400 Series", "PA-5450", "PA-7000 Series"
Protocols*	"TCP", "UDP", "IPv4", "IPv6", "TLS", "SSH", "HTTPS", "IPsec."

*When searching public vulnerability databases for Protocols, the evaluation team included the vendor name to narrow results.

A public search was performed on June 30, 2026 using the same search terms as identified in Table 3 for new vulnerabilities that might affect the TOE since the evaluation was completed on 17-Sep-2024, but replacing "PAN-OS 11.1" with "PAN-OS 11.2." Additionally, the KEV database was added to the list of searched databases:

- CISA Known Exploited Vulnerabilities (KEV) Catalog

Search Results:

In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version updates as shown in Table 4, which only shows search terms with results. Results returned by the new search that are dated before or on 17-Sep-2024 were tracked and evaluated in the original submission, and are therefore excluded from the current search.

Table 4 – Vulnerabilities that may affect the PAN-OS 11.2 TOE

VULNERABILITIES THAT MAY AFFECT THE PAN-OS 11.2 TOE		
Search Term	**Number of Results**	**Analysis**
"MIPS64"	**NVD Results**: One (1) **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	This search returned one (1) result, published prior to September 17, 2024.
"Zen 2"	**NVD Results**: Seventy-Three (73) Total' Fifty-Five (55) published prior to 17-Sep-2024 **US Cert Results**: One (1) Total, One (1) published prior to 17-Sep-2024 **TippingPoint ZDI Results**: Zero (0) Total	The TOE was **not** Vulnerable to the remaining eighteen (18) results
"Zen 3"	**NVD Results**: Fifty-Six (56) Total, Forty-Nine (49) published prior to 17-Sep-2024, Three (3) already reported for "Zen-2" **US Cert Results**: Four (4) Total, Four (4) published prior to 17-Sep-2024 **TippingPoint ZDI Results**: Zero (0) Total	The TOE was **not** Vulnerable to the remaining four (4) results
"Denverton"	**NVD Results**: One (1) **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	This search returned one (1) result, published prior to September 17, 2024.
"Tremont"	**NVD Results**: One (1) **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	This search returned one (1) result, published prior to September 17, 2024.

VULNERABILITIES THAT MAY AFFECT THE PAN-OS 11.2 TOE		
Search Term	**Number of Results**	**Analysis**
"Skylake"	**NVD Results**: One (1) **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was determined **not** vulnerable to CVE-2022-49124
"Ice Lake"	**NVD Results**: Three (3) Total, One (1) published prior to 17-Sep-2024 **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was **not** vulnerable to the remaining two (2) results.
"Broadwell"	**NVD Results**: Three (3) Total, Three (3) published prior to 17-Sep-2024 **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	This search returned three (3) results, published prior to September 17, 2024
"PAN-OS 11.2"	**NVD Results**: Two (2) Total **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was **not** vulnerable to the remaining two (2) results.
"Palo Alto Firewall"	**NVD Results**: Sixty-Five (65) Total, Thirty (30) published prior to 17-Sep-2024 **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was **not** vulnerable to the remaining thirty-five (35) results.
"Palo Alto Networks" under "Vendor/Project"	**KEV Results**: Fifteen (15) Total; Three (3) related to the "Expedition" migration tool and not to PAN-OS; Seven (7) already covered by other searches in this table;	The TOE was **not** vulnerable to the remaining five (5) results.

VULNERABILITIES THAT MAY AFFECT THE PAN-OS 11.2 TOE		
Search Term	**Number of Results**	**Analysis**
"Palo Alto Networks Firewall"	**NVD Results**: Sixty-Five (65) Total, Thirty (30) published prior to 17-Sep-2024, Thirty-Five (35) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Results identical to those for search term "Palo Alto Firewall"
"PA-400 Series"	**NVD Results**: One (1) Total, one (1) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "Palo Alto Firewall"
"PA-800 Series"	**NVD Results**: Two (2) Total, one (1) already reported for "PAN-OS 11.2" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "PAN-OS 11.2"
"PA-1400 Series"	**NVD Results**: One (1) Total, one (1) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "Palo Alto Firewall"
"PA-3200 Series"	**NVD Results**: Two (2) Total, one (1) published prior to 17-Sep-2024, one (1) already reported for "PAN-OS 11.2" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "PAN-OS 11.2"

VULNERABILITIES THAT MAY AFFECT THE PAN-OS 11.2 TOE		
Search Term	**Number of Results**	**Analysis**
"PA-3400 Series"	**NVD Results**: One (1) Total, one (1) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "Palo Alto Firewall"
"PA-5200 Series"	**NVD Results**: Two (2) Total, one (1) published prior to 17-Sep-2024, one (1) already reported for "PAN-OS 11.2" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "PAN-OS 11.2"
"PA-5400 Series"	**NVD Results**: Three (3) Total, Two (2) published prior to 17-Sep-2024, One (1) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "Palo Alto Firewall"
"PA-7000 Series"	**NVD Results**: Five (5) Total, four (4) published prior to 17-Sep-2024, one (1) already reported for "PAN-OS 11.2" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "PAN-OS 11.2"
"Palo Alto TCP"	**NVD Results**: Two (2) Total, two (2) published prior to 17-Sep-2024 **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	This search returned two (2) results, published prior to September 17, 2024.

VULNERABILITIES THAT MAY AFFECT THE PAN-OS 11.2 TOE		
Search Term	**Number of Results**	**Analysis**
"Palo Alto ipv6"	**NVD Results**: One (1) Total **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was determined **not** vulnerable to CVE-2026-0243
"Palo Alto TLS"	**NVD Results**: Two (2) Total, two (2) published prior to 17-Sep-2024 **US Cert Results**: One (1) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was determined **not** vulnerable to VU#521113
"Palo Alto SSH"	**NVD Results**: Three (3) Total, one (1) published prior to 17-Sep-2024, One (1) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was determined **not** vulnerable to the remaining issue: CVE-2025-0115
"Palo Alto HTTPS"	**NVD Results**: Twenty (20) Total, one (1) published prior to 17-Sep-2024, Seven (7) already reported for "Palo Alto Firewall", one (1) already reported for "pan-os 11.2", one (1) already reported for "Palo Alto SSH" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	The TOE was **not** vulnerable to the remaining ten (10) results.
"Palo Alto IPsec"	**NVD Results**: One (1) Total, one (1) already reported for "Palo Alto Firewall" **US Cert Results**: Zero (0) Total **TippingPoint ZDI Results**: Zero (0) Total	Covered in results for search term "Palo Alto Firewall"

Palo Alto Networks Security Advisories:
Palo Alto Networks published sixty-two (62) security advisories related to the PAN-OS, thirty-eight (38) of which were also returned by the searches in Table 4. The TOE was determined to not be vulnerable to the issues addressed in the remaining twenty-four (24) advisories.

Summary of All Changes to the TOE:
Table 5 is a summary of all the above changes, in terms of source/type of change, number of changes and their impact analysis rationale. Note that all the changes had minor security impact on the TOE.

Table 5– Summary of All Changes to the TOE

Source/Type of Changes	# of Changes	Impact analysis rationale summary
New Features	Forty-Four (44)	**Minor**: The added features improve usability or add capability without affecting evaluated security functionality.
Addressed Issues	Sixteen Hundred and two (1,602)	**Minor Changes** – Improved capability, capacity, usability, reliability, performance, problem determination, or corrected product behavior without affecting security functionality; or applied only to Panorama, not PAN-OS; or applied to the use of Features or Services, which were excluded from the evaluated configuration; or applied to the console or HTTP which are disabled in the evaluated configuration; or applied to Configurations, Appliances, and Subscriptions, which are not in the TOE; or were hot-fixes made to address possible security vulnerabilities, improving security posture without affecting security functionality.
New Hardware	One additional Variant: PA-455-5G	**Minor:** The PA-455-5G is equivalent to the PA-450R and PA-450-5G having the same number and type of ports and the same processor.

Equivalency Discussion:
Palo Alto Networks, Inc. initiated this maintenance action to address added features, issues, and new vulnerabilities present in software version upgrades to the PAN-OS TOE since its evaluation completed. Palo Alto added forty-four new features to the TOE and addressed sixteen hundred and two issues, all having minor impact. Palo Alto addressed all new vulnerabilities in sixty-two Palo Alto Networks Security Advisories, and determined that the TOE was not vulnerable to all other discovered and applicable CVEs. Palo Alto Networks, inc. also performed regression testing of the entire TOE to ensure that the TOE continued to perform as expected at the time of the original evaluation after new features were added and issue changes applied. Vendor regression testing,

comprising execution of automation test suites and additional manual testing, produced test results consistent with the previous test results.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.