SASSURANCE CONTINUITY MAINTENANCE REPORT FOR PALO ALTO NETWORKS GLOBALPROTECT APP 6

Maintenance Update of Palo Alto Networks GlobalProtect App 6

Maintenance Report Number: CCEVS-VR-VID11402-2025

Date of Activity: 31 Oct 2025

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 GlobalProtect App 6

Impact Analysis Report, Version 1.1, October 27, 2025

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

Security Target: Palo Alto Networks GlobalProtect App 6 Security Target, Version 1.0, July 26, 2023. Changes in the Security Target are:

- Security Target updated to Palo Alto Networks GlobalProtect App 6 Security Target, Version 1.1, September 2025.
- Section 1.1 – updated ST and TOE identification
- Section 2.3 – Updated TOE documentation references
- Section 5.2.6 – FPT_LIB_EXT.1.1 updated to identify third party libraries omitted from original ST
- Section 6.6 – updated identification of TOE install packages in relation to FPT_TUD_EXT.1 and FPT_TUD_EXT.2
- Section 6.6 – updated list of third party libraries associated with each platform version of TOE.

Common Criteria Compliance Guide: Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) GlobalProtect 6 App, Revision Date: June 28, 2023. Changes in the CCECG are:

- CCECG updated to Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) GlobalProtect 6 App, Revision Date: September 8, 2025.
- "Document Purpose and Scope" – updated guidance references
- "Scope of Evaluation" – Updated TOE identification

- "Software Download and Installation" – Updated version number for Windows, Linux, and macOS versions of TOE.

User Guide: Changes were made to the GlobalProtect App User Guide, Version 6.0, Revision Date: January 24, 2023, including:

- User Guide updated to GlobalProtect App User Guide, Version 6.1, Revision Date: March 29, 2023.
  - This guide covers Android and iOS.
  - Added iOS subsections "Connect for the First Time", "Connect with the On-Demand Method", "Connect with Always-On Connection Method."
- User Guide updated to GlobalProtect App User Guide, Version 6.2, Revision Date: May 19, 2023.
  - This guide covers Linux.
  - Added subsections "Install the CLI Version of GlobalProtect for Linux for RPM Based Distros", "Install the CLI Version of GlobalProtect for Linux for Debian Based Distros", "Support for Native Certificate Store for Prisma Access and GlobalProtect App."
- User Guide updated to GlobalProtect App User Guide, Version 6.3, Revision Date: October 24, 2024.
  - This guide covers Windows and macOS.
  - Added section "Reveal Password on Windows Logon Screen for GlobalProtect."

Admin Guide: Palo Alto Networks GlobalProtect Administrator's Guide, Version 10.1, Revision Date: February 22, 2022. Changes in the Admin Guide are:

- Admin Guide updated to GlobalProtect Administrator's Guide, Version 10.1, Revision Date: June 11, 2025.
- Added sections "Replace an Expired GlobalProtect Portal or Gateway Certificate", "Support for Native Certificate Store for Prisma Access and GlobalProtect App on Linux Endpoints", "Set Up Cloud Identity Engine Authentication", "DHCP Based IP Address Assignment and Management for GlobalProtect", "GlobalProtect Processes to be Whitelisted on EDR Deployments."

TOE software: Updated from version 6.0.7 to version 6.3.3 for Windows, macOS, and Linux, and version 6.0.13 for Android and iOS.

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 September 2025. 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 software updates adding features that do not affect the evaluated security functionality. An updated public vulnerability search was performed on October 27, 2025, 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 software from the evaluated version 6.0.7 (Table 1) through three versions, 6.1 (Table 2), 6.2 (Table 3), and 6.3 (Table 4), respectively adding new features for Android and iOS, Linux, and finally, Windows and macOS. The feature additions did not affect the security claims in the Palo Alto Networks GlobalProtect App 6 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.

Table 1 – Features Introduced in GlobalProtect 6.0 (post 6.0.7)

FEATURES INTRODUCED IN GLOBALPROTECT 6.0 (POST 6.0.7)	
Feature	**Analysis**
Version 6.0.9: Embedded Browser Framework Upgrade	Minor: This feature improves usability without affecting evaluated security functionality.
Version 6.0.9: Deploy Certificates for Authentication to the Endpoint Without Using Mobile Device Management (MDM)	Minor: This feature improves usability without affecting evaluated security functionality.
Version 6.0.9: Enhanced GlobalProtect App Log Sharing Functionality	Minor: This feature improves usability without affecting evaluated security functionality.

Table 2 – Features Introduced in GlobalProtect 6.1

FEATURES INTRODUCED IN GLOBALPROTECT 6.1	
Feature	**Analysis**
Advanced Internal Host Detection	Minor: This feature adds capability without affecting evaluated security functionality.

FEATURES INTRODUCED IN GLOBALPROTECT 6.1	
Feature	**Analysis**
Proxy Auto Configuration (PAC) Deployment from GlobalProtect	Minor: This feature improves usability without affecting evaluated security functionality.
End-user Notification about GlobalProtect Session Logout	Minor: This feature improves usability without affecting evaluated security functionality.
Simplified and Seamless macOS GlobalProtect App Deployment Using Jamf MDM Integration	Minor: This feature improves usability without affecting evaluated security functionality.
New Linux OS Support for Ubuntu	Minor: The TOE is evaluated on Linux Ubuntu 20.04.
New Linux OS Support for Red Hat Enterprise Linux (RHEL)	Minor: The TOE is evaluated on Linux Ubuntu 20.04.
Split DNS and Split Domain (Linux OS)	Minor: This feature adds capability to the TOE on Linux platforms without affecting evaluated security functionality.
Deploy the GlobalProtect App for iOS using Jamf Pro	Minor: This feature improves usability without affecting evaluated security functionality.
Version 6.1.5 (iOS and Android): Embedded Browser Framework Upgrade	Minor: This feature improves usability without affecting evaluated security functionality.
Version 6.1.5 (iOS and Android): Share Sheet Support	Minor: This feature improves usability without affecting evaluated security functionality.

Table 3 – Features Introduced in GlobalProtect 6.2

FEATURES INTRODUCED IN GLOBALPROTECT 6.2	
Feature	**Analysis**
Conditional Connect Method for GlobalProtect	Minor: This feature improves usability without affecting evaluated security functionality.
Enhanced Split Tunnel Configuration	Minor: This feature adds capability to the TOE without affecting evaluated security functionality.
Prisma Access Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security	Minor: This feature adds capability to the TOE without affecting evaluated security functionality.
Host Information Profile (HIP) Exceptions for Patch Management	Minor: This feature improves usability without affecting evaluated security functionality.
Host Information Profile (HIP) Process Remediation	Minor: This feature improves usability without affecting evaluated security functionality.
Support for Native Certificate Store for Linux Endpoints	Minor: This feature adds capability to the TOE without affecting evaluated security functionality.
Extend User Session for GlobalProtect Users	Minor: This feature improves usability without affecting evaluated security functionality.
Version 6.2.3: Embedded Browser Framework Upgrade	Minor: This feature improves usability without affecting evaluated security functionality.

Table 4 – Features Introduced in GlobalProtect 6.3

FEATURES INTRODUCED IN GLOBALPROTECT 6.3	
Feature	**Analysis**
Enhanced HIP Remediation Process Improvements	Minor: This feature improves usability without affecting evaluated security functionality.
Enhancements for Authentication Using Smart Cards – Removal of Multiple PIN Prompts	Minor: This feature improves usability without affecting evaluated security functionality.
Enhancements for Authentication Using Smart Cards – Authentication Fallback	Minor: This feature improves usability without affecting evaluated security functionality.
Intelligent Portal	Minor: This feature improves usability without affecting evaluated security functionality.
Connect to GlobalProtect App with IPSec Only	This feature adds capability to the TOE without affecting evaluated security functionality.
Embedded Browser Framework Upgrade	Minor: This feature improves usability without affecting evaluated security functionality.
GlobalProtect Best Gateway Selection	Minor: This feature improves usability without affecting evaluated security functionality.
Wildcard Support for Split Tunnel Settings Based on the Application	This feature adds capability to the TOE without affecting evaluated security functionality.
Enhancements for Authentication Using Smart Cards	Minor: This feature improves usability without affecting evaluated security functionality.
Improvements for Multi Authentication CIE Experience	Minor: This feature improves usability without affecting evaluated security functionality.
Version 6.3.1: Intelligent Internal Host Detection	Minor: This feature improves usability without affecting evaluated security

FEATURES INTRODUCED IN GLOBALPROTECT 6.3	
Feature	**Analysis**
	functionality.

Addressed Issues:
In addition to the new features enumerated in Table 1, Table 2, Table 3, and Table 4, Palo Alto Networks addressed nine hundred and seventy (970) issues in releases 6.0 through 6.3. 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 5 from the full list available in the IAR.

Table 5 – Issues Addressed in GlobalProtect 6

ISSUES ADDRESSED IN GLOBALPROTECT 6		
GlobalProtect Version	**Number of Addressed Issues**	**Analysis**
6.0.8	Fifty-Five (55) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.0.10	Seventy-Seven (77) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.0.10-814 (Windows and macOS)	One (1) Issue Addressed	Minor Change – corrected product behavior without affecting security functionality.
6.0.10-c826 (Windows and macOS)	One (1) Issue Addressed	Minor Change – improved usability without affecting security functionality.
6.0.11 (Windows and macOS)	One (1) Issue Addressed	Minor Change – corrected product behavior without affecting security functionality.
6.0.12 (Android and iOS)	Three (3) Issues Addressed	Minor Changes – improved usability, or corrected product behavior without affecting security functionality.
6.0.13 (iOS)	One (1) Issue Addressed	Minor Change – corrected product behavior without affecting security functionality.

ISSUES ADDRESSED IN GLOBALPROTECT 6		
GlobalProtect Version	**Number of Addressed Issues**	**Analysis**
6.1.1 (Windows, macOS, and Linux)	Ten (10) Issues Addressed	Minor Changes – cosmetic or improved usability, reliability, or corrected product behavior without affecting security functionality.
6.1.2 (Windows and macOS)	One Hundred and Twenty (120) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.1.3 (Windows, macOS, and Linux)	Fifty (50) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.1.4 (Windows, macOS, iOS, Android, and Linux)	Twenty-Five (25) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.1.5 (Linux)	Eight (8) Issues Addressed	Minor Changes – improved usability or reliability without affecting security functionality.
6.1.5 (iOS)	One (1) Issue Addressed	Minor Change – improved reliability without affecting security functionality.
6.1.5 (Windows and macOS)	Fifty (50) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.1.5 (Android)	One (1) Issue Addressed	Minor Change – improved usability without affecting security functionality.
6.2.0 (Linux)	Ten (10) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.1 (Windows and macOS)	Forty-Eight (48) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.

ISSUES ADDRESSED IN GLOBALPROTECT 6		
GlobalProtect Version	**Number of Addressed Issues**	**Analysis**
6.2.1 (Linux)	Thirteen (13) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.2 (Windows and macOS)	Eight (8) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.3 (Windows and macOS)	Seventy-Six (76) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.4 (Windows and macOS)	Seventy-Two (72) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.5 (Windows and macOS)	Fifty-Three (53) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.6 (Windows and macOS)	Twenty-Three (23) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.6 (Linux)	Eighteen (18) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.2.7 (Windows and macOS)	Ten (10) Issues Addressed	Minor Changes – improved usability or reliability without affecting security functionality.
6.2.8 (Windows and macOS)	Fifty-Three (53) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.3.1	Forty-Two (42) Issues Addressed	Minor Changes – improved usability, reliability, or corrected product behavior without affecting security functionality.
6.3.1-c383	Six (6) Issues Addressed	Minor Changes – improved usability or reliability without affecting security functionality.

ISSUES ADDRESSED IN GLOBALPROTECT 6		
GlobalProtect Version	**Number of Addressed Issues**	**Analysis**
6.3.2	Forty-Seven (47) Issues Addressed	Minor Changes – improved performance, usability, usability in non-FIPS-CC mode, reliability, or corrected product behavior without affecting security functionality.
6.3.3	Eighty-Seven (87) Issues Addressed	Minor Changes – improved performance, usability, reliability, or corrected product behavior without affecting security functionality.

Vulnerability Searches:

A public search was performed on October 27, 2025 for new vulnerabilities that might affect the TOE since the evaluation was completed. 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 6.

Table 6 – Vulnerabilities that may affect the GlobalProtect TOE

VULNERABILITIES THAT MAY AFFECT THE GLOBALPROTECT 6 TOE		
Search Term	**Number of Results**	**Analysis**
"Palo Alto Networks"	Search produced Two hundred and seventy (270) results returned with 154 published prior to 28 August 2023. 100 of the remaining 116 results were not applicable to the TOE, leaving sixteen (16) CVEs.	The TOE was determined to not be vulnerable these sixteen Common Vulnerabilities and Exposures (CVEs): CVE-2025-4232, CVE-2025-4227, CVE-2025-2183, CVE-2025-2179, CVE-2025-0141, CVE-2025-0140, CVE-2025-0135, CVE-2025-0131, CVE-2025-0120, CVE-2025-0118, CVE-2024-5921, CVE-2024-9473, CVE-2024-5915, CVE-2024-5908, CVE-2024-2432, CVE-2024-2431
"GlobalProtect"	Search produced 74 results, 46 of which were published prior to 28 August 2023. Of the 28 results published since 28 August 2023, 11 results applied to products other than the TOE. Of the remaining 17 results, 16 were also returned by the search on "Palo Alto Networks" and are reported in the previous row of this table.	The TOE was determined to not be vulnerable CVE-2025-0117
"VPN Client"	Search returned 204 results, 163 of which were published prior to 28 August 2023. Of the 41 results published since 28 August 2023, 40 results applied to products other than the TOE.	The TOE was determined to not be vulnerable CVE-2024-3661
"OPENSSL	Search produced 28	The TOE was determined to not be vulnerable CVE-2025-

VULNERABILITIES THAT MAY AFFECT THE GLOBALPROTECT 6 TOE		
Search Term	**Number of Results**	**Analysis**
1.1.1"	results, 26 of which were published prior to 28 August 2023.	4575 or CVE-2025-34203
"COMMONS COMPRESS"	The Android version of the TOE uses Apache Commons Compress 1.5. This search produced 8 CVE results.	The TOE was determined to not be vulnerable these eight CVEs: CVE-2024-26308, CVE-2024-25710, CVE-2023-42503, CVE-2021-21251, CVE-2019-12402, CVE-2018-1324, CVE-2018-11771, CVE-2012-2098
"webview2"	The Windows version of the TOE uses the Microsoft Webview2 library (Microsoft.Web.WebView2), version 1.0.2088.41. This search produced three CVE results.	The TOE was determined to not be vulnerable these three CVEs: CVE-2024-29049, CVE-2023-24892, CVE-2023-22880

Palo Alto Networks Security Advisories:

Palo Alto Networks published twenty-one (21) security advisories related to the GlobalProtect App, seventeen (17) of which were also returned by the searches in Table 6. The TOE was determined to not be vulnerable to these remaining four CVEs: CVE-2024-47076, CVE-2024-8687, CVE-2024-3094, CVE-2023-44487.

Summary of All Changes to the TOE:

Table 7 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 7– Summary of All Changes to the TOE

Source/Type of Changes	# of Changes	Impact analysis rationale summary
New Features	Thirty-Two (32)	Minor: The added features improve usability or add capability without affecting evaluated security functionality.
Addressed Issues	Nine Hundred and Seventy (970)	Minor Changes – cosmetic or improved usability, reliability, or corrected product behavior without affecting security functionality.

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 GlobalProtect App 6 TOE since its evaluation completed. Palo Alto added thirty-two new features to the TOE and addressed nine hundred and seventy issues, all having minor impact. Palo Alto addressed all new vulnerabilities in twenty-one 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.