SSA-354569: Multiple Vulnerabilities in Palo Alto Networks PAN-OS on RUGGEDCOM APE1808 Devices

Publication Date: 2024-11-22
Last Update: 2025-06-10
Current Version: V1.5
CVSS v3.1 Base Score: 10.0
CVSS v4.0 Base Score: 9.3

SUMMARY

Palo Alto Networks has published [1] information on vulnerabilities in PAN-OS. This advisory lists the related Siemens Industrial products affected by these vulnerabilities.

Siemens is preparing fix versions and recommends countermeasures for products where fixes are not, or not yet available.

[1] https://security.paloaltonetworks.com/

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808:	See below See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW on which you configured a GlobalProtect gateway affected by CVE-2024-2550	Upgrade Palo Alto Networks Virtual NGFW V11.1.8. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW affected by CVE-2024-0012, CVE-2024-2552, CVE-2024-9474, CVE-2025-0108, CVE-2025-0109, CVE-2025-0111, CVE-2025-0115, CVE-2025-0123, CVE-2025-0124, CVE-2025-0125, CVE-2025-0128, CVE-2025-0137	Upgrade Palo Alto Networks Virtual NGFW V11.1.8. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW with DNS Security logging enabled either with a DNS Security License or an Advanced DNS Security License affected by CVE-2024-3393	Upgrade Palo Alto Networks Virtual NGFW V11.1.8. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with PAN-OS OpenConfig Plugin affected by CVE-2025-0110	Follow the remediation available in Palo Alto Networks' Security Advisory See further recommendations from section Workarounds and Mitigations

RUGGEDCOM APE1808: All versions with LLDP enabled on at least one network interface with "Mode" configured to "transmit-receive" or "receive-only" affected by CVE-2025-0116	Upgrade Palo Alto Networks Virtual NGFW V11.1.8. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW on which user configured a GlobalProtect portal to use SAML Authentication affected by CVE-2025-0126	Upgrade Palo Alto Networks Virtual NGFW V11.1.8. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW with web proxy feature enabled affected by CVE-2025-0130	Upgrade Palo Alto Networks Virtual NGFW V11.1.8. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- CVE-2024-0012: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2024-3393: For upstream mitigation measures, refer to Palo Alto Networks' Security Advisory
- CVE-2024-9474: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2025-0108: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2025-0109: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2025-0110: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2025-0111: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2025-0115: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory
- CVE-2025-0124: Exposure can be reduced by restricting access to a jump box that is the only system allowed to access the management interface. This ensures that attacks can succeed only if they obtain privileged access through those specified internal IP addresses Palo Alto Networks' Security Advisory
- CVE-2025-0125: Exposure can be reduced by restricting access to a jump box that is the only system allowed to access the management interface. This will ensure that attacks can succeed only if they obtain privileged access through those specified IP addresses Palo Alto Networks' Security Advisory
- CVE-2025-0130: Disable web proxy feature if not necessary. Palo Alto Networks' Security Advisory
- CVE-2025-0137: Exposure can be reduced by restricting access to a jump box that is the only system allowed to access the management interface. This will ensure that attacks can succeed only if they obtain privileged access through those specified IP addresses Palo Alto Networks' Security Advisory

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

RUGGEDCOM APE1808 is a powerful utility-grade application hosting platform that lets you deploy a range of commercially available applications for edge computing and cybersecurity in harsh, industrial environments.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-0012

An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:N/SA:N
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2024-2550

A null pointer dereference vulnerability in the GlobalProtect gateway in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to stop the GlobalProtect service on the firewall by sending a specially crafted packet that causes a denial of service (DoS) condition. Repeated attempts to trigger this condition result in the firewall entering maintenance mode.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2024-2552

A command injection vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to bypass system restrictions in the management plane and delete files on the firewall.

CVSS v3.1 Base Score	6.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H
CVSS v4.0 Base Score	6.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2024-3393

A Denial of Service vulnerability in the DNS Security feature of Palo Alto Networks PAN-OS software allows an unauthenticated attacker to send a malicious packet through the data plane of the firewall that reboots the firewall. Repeated attempts to trigger this condition will cause the firewall to enter maintenance mode.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2024-9474

A privilege escalation vulnerability in Palo Alto Networks PAN-OS software allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2025-0108

An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v4.0 Base Score	8.8
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2025-0109

An unauthenticated file deletion vulnerability in the Palo Alto Networks PAN-OS management web interface enables an unauthenticated attacker with network access to the management web interface to delete certain files as the "nobody" user; this includes limited logs and configuration files but does not include system files.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
CWE	CWE-73: External Control of File Name or Path

Vulnerability CVE-2025-0110

A command injection vulnerability in the Palo Alto Networks PAN-OS OpenConfig plugin enables an authenticated administrator with the ability to make gNMI requests to the PAN-OS management web interface to bypass system restrictions and run arbitrary commands. The commands are run as the "__openconfig" user (which has the Device Administrator role) on the firewall.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.6
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2025-0111

An authenticated file read vulnerability in the Palo Alto Networks PAN-OS software enables an authenticated attacker with network access to the management web interface to read files on the PAN-OS filesystem that are readable by the "nobody" user.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	7.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-73: External Control of File Name or Path

Vulnerability CVE-2025-0115

A vulnerability in the Palo Alto Networks PAN-OS software enables an authenticated admin on the PAN-OS CLI to read arbitrary files.

The attacker must have network access to the management interface (web, SSH, console, or telnet) and successfully authenticate to exploit this issue.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	6.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-41: Improper Resolution of Path Equivalence

Vulnerability CVE-2025-0116

A Denial of Service (DoS) vulnerability in Palo Alto Networks PAN-OS software causes the firewall to unexpectedly reboot when processing a specially crafted LLDP frame sent by an unauthenticated adjacent attacker. Repeated attempts to initiate this condition causes the firewall to enter maintenance mode.

CVSS v3.1 Base Score	5.7
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	6.8
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2025-0123

A vulnerability in the Palo Alto Networks PAN-OS software enables unlicensed administrators to view clear-text data captured using the packet capture feature in decrypted HTTP/2 data streams traversing network interfaces on the firewall. HTTP/1.1 data streams are not impacted.

CVSS v3.1 Base Score	6.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N
CVSS v4.0 Base Score	5.9
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N
CWE	CWE-312: Cleartext Storage of Sensitive Information

Vulnerability CVE-2025-0124

An authenticated file deletion vulnerability in the Palo Alto Networks PAN-OS® software enables an authenticated attacker with network access to the management web interface to delete certain files as the “nobody” user; this includes limited logs and configuration files but does not include system files.

CVSS v3.1 Base Score	3.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
CVSS v4.0 Base Score	5.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N
CWE	CWE-73: External Control of File Name or Path

Vulnerability CVE-2025-0125

An improper input neutralization vulnerability in the management web interface of the Palo Alto Networks PAN-OS software enables a malicious authenticated read-write administrator to impersonate another legitimate authenticated PAN-OS administrator.

CVSS v3.1 Base Score	5.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N
CWE	CWE-83: Improper Neutralization of Script in Attributes in a Web Page

Vulnerability CVE-2025-0126

When configured using SAML, a session fixation vulnerability in the GlobalProtect™ login enables an attacker to impersonate a legitimate authorized user and perform actions as that GlobalProtect user. This requires the legitimate user to first click on a malicious link provided by the attacker.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:H
CVSS v4.0 Base Score	8.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:H/SC:H/SI:N/SA:N
CWE	CWE-384: Session Fixation

Vulnerability CVE-2025-0128

A denial-of-service (DoS) vulnerability in the Simple Certificate Enrollment Protocol (SCEP) authentication feature of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to initiate system reboots using a maliciously crafted packet. Repeated attempts to initiate a reboot causes the firewall to enter maintenance mode.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2025-0130

A missing exception check in Palo Alto Networks PAN-OS® software with the web proxy feature enabled allows an unauthenticated attacker to send a burst of maliciously crafted packets that causes the firewall to become unresponsive and eventually reboot. Repeated successful attempts to trigger this condition will cause the firewall to enter maintenance mode.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.2
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2025-0137

An improper input neutralization vulnerability in the management web interface of the Palo Alto Networks PAN-OS® software enables a malicious authenticated read-write administrator to impersonate another legitimate authenticated PAN-OS administrator.

CVSS v3.1 Base Score	3.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N
CVSS v4.0 Base Score	4.8
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CWE	CWE-83: Improper Neutralization of Script in Attributes in a Web Page

ADDITIONAL INFORMATION

Customers are advised to consult and implement the workarounds provided in Palo Alto Networks' upstream security notifications [1]. PANW provides a public RSS feed for their security alerts to which customers can also subscribe [2].

[1] https://security.paloaltonetworks.com

[2] https://security.paloaltonetworks.com/rss.xml

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-11-22):	Publication Date
V1.1 (2025-02-11):	Added CVE-2024-3393 that affects RUGGEDCOM APE1808 devices with Palo Alto Networks Virtual NGFW with DNS Security logging enabled either with a DNS Security License or an Advanced DNS Security License
V1.2 (2025-02-19):	Added CVE-2025-0108, CVE-2025-0109, CVE-2025-0110 and CVE-2025-0111
V1.3 (2025-04-08):	Added CVE-2025-0115 and CVE-2025-0116. Updated remediation for RUGGEDCOM APE1808
V1.4 (2025-05-13):	Added CVE-2025-0123, CVE-2025-0124, CVE-2025-0125, CVE-2025-0126 and CVE-2025-0128
V1.5 (2025-06-10):	Added CVE-2025-0130 and CVE-2025-0137

TERMS OF USE