SSA-354569: Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices

Publication Date: 2024-11-22
Last Update: 2024-11-22
Current Version: V1.0
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:	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 you configured a GlobalProtect gateway affected by CVE-2024-2550	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	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-2024-9474: Exposure can be reduced by limiting access to the management interface to trusted internal IP addresses as described in Palo Alto Networks' Security Advisory

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. 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

The 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-2024-9474

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')

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

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.