SSA-455250: Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 devices

Publication Date: 2024-04-09
Last Update: 2024-04-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 8.2

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 updates and recommends specific countermeasures for products where updates are not, or not yet available. Customers are advised to consult and implement the workarounds provided in Palo Alto Networks' upstream security notifications.

[1] https://security.paloaltonetworks.com/?version=11.0.1&product=PAN-OS

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW configured with support for the CHACHA20-POLY1305 algorithm or any Encrypt-then-MAC algorithms affected by CVE-2023-48795	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW affected by CVE-2023-6789, CVE-2023-6793, CVE-2024-0008	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 that are configured with BGP routing features enabled affected by CVE-2023-38802	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-2023-48795: Customers can resolve this issue by configuring the in-use SSH profile to contain at least one cipher and at least one MAC algorithm, which removes support for CHACHA20-POLY1305 and all Encrypt-then-MAC algorithms available (ciphers with -etm in the name) in PAN-OS software. See Palo Alto Networks' upstream documentation https://security.paloaltonetworks.com/CVE-2023-48795 for additional guidance

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-2023-6789

A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a malicious authenticated read-write administrator to store a JavaScript payload using the web interface. Then, when viewed by a properly authenticated administrator, the JavaScript payload executes and disguises all associated actions as performed by that unsuspecting authenticated administrator.

CVSS v3.1 Base Score	4.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	5.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2023-6793

An improper privilege management vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to revoke active XML API keys from the firewall and disrupt XML API usage.

CVSS v3.1 Base Score	2.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
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:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2023-38802

FRRouting FRR 7.5.1 through 9.0 and Pica8 PICOS 4.3.3.2 allow a remote attacker to cause a denial of service via a crafted BGP update with a corrupted attribute 23 (Tunnel Encapsulation)

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/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2023-48795

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust; and there could be effects on Bitvise SSH through 9.31.

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:H/A:N/E:P/RL:O/RC:C
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:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-222: Truncation of Security-relevant Information

Vulnerability CVE-2024-0008

Web sessions in the management interface in Palo Alto Networks PAN-OS software do not expire in certain situations, making it susceptible to unauthorized access.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-613: Insufficient Session Expiration

ADDITIONAL INFORMATION

Customers are advised to consult and implement the workarounds provided in Palo Alto Networks' upstream security notifications [1].

[1] https://security.paloaltonetworks.com/?version=11.0.1&product=PAN-OS

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 (2024-04-09): Publication Date

TERMS OF USE