SSA-822518: Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW before V11.0.1 on RUGGEDCOM APE1808 devices

Publication Date: 2024-04-09
Last Update: 2024-04-09
Current Version: V1.0
CVSS v3.1 Base Score: 8.8
CVSS v4.0 Base Score: 7.5

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=10.2.2&product=PAN-OS

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW before V11.0.1 affected by all CVEs	Upgrade Palo Alto Networks Virtual NGFW V11.0.1. Contact Siemens customer support to receive patch and update information.

WORKAROUNDS AND MITIGATIONS

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-2022-0028

A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-406: Insufficient Control of Network Message Volume (Network Amplification)

Vulnerability CVE-2023-0005

A vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to expose the plaintext values of secrets stored in the device configuration and encrypted API keys.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

Vulnerability CVE-2023-0008

A file disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-write administrator with access to the web interface to export local files from the firewall through a race condition.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-73: External Control of File Name or Path

Vulnerability CVE-2023-6790

A DOM-Based cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a remote attacker to execute a JavaScript payload in the context of an administrator's browser when they view a specifically crafted link to the PAN-OS web interface.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.5
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2023-6791

A credential disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to obtain the plaintext credentials of stored external system integrations such as LDAP, SCP, RADIUS, TACACS+, and SNMP from the web interface.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	6.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N
CWE	CWE-522: Insufficiently Protected Credentials

Vulnerability CVE-2023-38046

A vulnerability exists in Palo Alto Networks PAN-OS software that enables an authenticated administrator with the privilege to commit a specifically created configuration to read local files and resources from the system.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-610: Externally Controlled Reference to a Resource in Another Sphere

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=10.2.2&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

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.