SSA-750274: Impact of CVE-2024-3400 on RUGGEDCOM APE1808 devices configured with Palo Alto Networks Virtual NGFW

Publication Date: 2024-04-19
Last Update: 2024-04-19
Current Version: V1.0
CVSS v3.1 Base Score: 10.0
CVSS v4.0 Base Score: 10.0

SUMMARY

Palo Alto Networks has published [1] information on CVE-2024-3400 in PAN-OS. This advisory addresses Siemens Industrial products affected by this vulnerability.

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/CVE-2024-3400

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW configured with GlobalProtect gateway or GlobalProtect portal (or both). affected by all CVEs	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:

- Disable GlobalProtect gateway and GlobalProtect portal; note that these features are disabled by default in RUGGEDCOM APE1808 deployments
- Customers with a Threat Prevention subscription can block attacks for this vulnerability using Threat IDs 95187, 95189, and 95191 (available in Applications and Threats content version 8836-8695 and later). For further instruction see Palo Alto Network's upstream notification (https://security.paloaltonetworks.com/CVE-2024-3400)

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-2024-3400

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

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/E:H/RL:T/RC:C
CVSS v4.0 Base Score	10.0
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

ADDITIONAL INFORMATION

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

[1] https://security.paloaltonetworks.com/CVE-2024-3400

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 (2024-04-19): 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.