SSA-698820: Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 devices

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

Fortinet has published information on vulnerabilities in FORTIOS. This advisory lists the related Siemens Industrial products.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available. Siemens recommends to consult and implement the workarounds provided in Fortinet's upstream security notifications.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808: All versions with Fortinet NGFW affected by all CVEs	Contact 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-2023-46720

A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2024-21754

A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file.

CVSS v3.1 Base Score	1.8
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-916: Use of Password Hash With Insufficient Computational Effort

Vulnerability CVE-2024-23111

A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’)

Vulnerability CVE-2024-26010

A stack-based buffer overflow in Fortinet FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiWeb, FortiAuthenticator, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.1 through 7.0.3, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specially crafted packets.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

ADDITIONAL INFORMATION

Siemens recommends to consult and implement the workarounds provided in Fortinet's upstream security notifications. Fortinet provides a public RSS feed for their security alerts to which customers can also subscribe [1].

[1] https://filestore.fortinet.com/fortiguard/rss/ir.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 (2024-07-09): Publication Date

TERMS OF USE