SSA-832273: Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 devices

Publication Date: 2024-03-12
Last Update: 2024-04-09
Current Version: V1.1
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 8.7

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 CVE-2023-38545, CVE-2023-38546, CVE-2023-44250, CVE-2023-44487, CVE-2023-46717, CVE-2023-47537, CVE-2024-21762, CVE-2024-23112, CVE-2024-23113	Update Fortigate NGFW to V7.4.3. Contact customer support to receive patch and update information. See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Fortinet NGFW with captive portal enabled affected by CVE-2023-42789, CVE-2023-42790	Update Fortigate NGFW to V7.4.3. 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-2023-42789, CVE-2023-42790: Set a non form-based authentication scheme (see https://fortiguard.fortinet.com/psirt/FG-IR-23-328)
- CVE-2024-21762: Disable SSL VPN (disable webmode is NOT a valid workaround) (see https://www.fortiguard.com/psirt/FG-IR-24-015)
- CVE-2024-23113: For each interface, remove the fgfm access (see https://www.fortiguard.com/psirt/FG-IR-24-029)

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-2023-38545

A heap-based buffer overflow vulnerability in the SOCKS5 proxy handshake in the Curl package. If Curl is unable to resolve the address itself, it passes the hostname to the SOCKS5 proxy. However, the maximum length of the hostname that can be passed is 255 bytes. If the hostname is longer, then Curl switches to the local name resolving and passes the resolved address only to the proxy. The local variable that instructs Curl to "let the host resolve the name" could obtain the wrong value during a slow SOCKS5 handshake, resulting in the too-long hostname being copied to the target buffer instead of the resolved address, which was not the intended behavior.

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-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-38546

This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met.

libcurl performs transfers. In its API, an application creates "easy handles" that are the individual handles for single transfers.

libcurl provides a function call that duplicates en easy handle called curl_easy_duphandle.

If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as `none` (using the four ASCII letters, no quotes).

Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named `none` - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-73: External Control of File Name or Path

Vulnerability CVE-2023-42789

A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2023-42790

A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/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-2023-44250

An improper privilege management vulnerability [CWE-269] in a Fortinet FortiOS HA cluster version 7.4.0 through 7.4.1 and 7.2.5 and in a FortiProxy HA cluster version 7.4.0 through 7.4.1 allows an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2023-44487

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

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
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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2023-46717

An improper authentication vulnerability [CWE-287] in FortiOS versions 7.4.1 and below, versions 7.2.6 and below, and versions 7.0.12 and below when configured with FortiAuthenticator in HA may allow a readonly user to gain read-write access via successive login attempts.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2023-47537

An improper certificate validation vulnerability in Fortinet FortiOS 7.0.0 - 7.0.13, 7.2.0 - 7.2.6 and 7.4.0 - 7.4.1 allows a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the FortiLink communication channel between the FortiOS device and FortiSwitch.

CVSS v3.1 Base Score	4.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2024-21762

A out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 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 specifically crafted requests

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2024-23112

An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-639: Authorization Bypass Through User-Controlled Key

Vulnerability CVE-2024-23113

A use of externally-controlled format string vulnerability [CWE-134] in FortiOS fgfmd daemon may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-134: Use of Externally-Controlled Format String

ADDITIONAL INFORMATION

Siemens recommends to consult and implement the workarounds provided in Fortinet's upstream security notifications.

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 (2024-03-12):	Publication Date
V1.1 (2024-04-09):	Added CVE-2023-42789, CVE-2023-42790, CVE-2023-46717, CVE-2024-23112 and updated remediations

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.