SSA-832273: Multiple Vulnerabilities in Fortigate NGFW before V7.4.3 on RUGGEDCOM APE1808 devices

Publication Date:	2024-03-12
Last Update:	2024-07-09
Current Version:	V1.4
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 has released a new version of Fortigate NGFW for RUGGEDCOM APE1808 and recommends to update to the latest version. 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:	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 < V7.4.3 affected by CVE-2023-36640, CVE-2023-38545, CVE-2023-38546, CVE-2023-41677, CVE-2023-44247, CVE-2023-44250, CVE-2023-44487, CVE-2023-45583, CVE-2023-45586, CVE-2023-46714, CVE-2023-46717, CVE-2023-47537, CVE-2023-48784, CVE-2024-21762, CVE-2024-23110, CVE-2024-23112, CVE-2024-23113, CVE-2024-23662, CVE-2024-26007	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 < V7.4.3 and 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-2023-36640

A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 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, FortiPAM versions 1.0.0 through 1.0.3, FortiOS versions 7.2.0, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.16 allows attacker to execute unauthorized code or commands via specially crafted 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-134: Use of Externally-Controlled Format String

Vulnerability CVE-2023-38545

This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake.

When curl is asked to pass along the hostname to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that hostname can be is 255 bytes.

If the hostname is detected to be longer than 255 bytes, curl switches to local name resolving and instead passes on the resolved address only to the proxy. Due to a bug, the local variable that means "let the host resolve the name" could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long hostname to the target buffer instead of copying just the resolved address there.

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
CWE	CWE-122: Heap-based Buffer Overflow

Product Specific Vulnerability Description

For the following products, the impact of the vulnerability is different.

RUGGEDCOM APE1808:

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:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C (6.7)

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-2023-41677

A insufficiently protected credentials in Fortinet 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, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17 allows attacker to execute unauthorized code or commands via targeted social engineering attack

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-522: Insufficiently Protected Credentials

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-2023-44247

A double free vulnerability [CWE-415] in Fortinet FortiOS before 7.0.0 may allow a privileged attacker to execute code or commands via crafted HTTP or HTTPs requests.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

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-2023-45583

A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.5, 7.0.0 through 7.0.11, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6 FortiPAM versions 1.1.0, 1.0.0 through 1.0.3 FortiOS versions 7.4.0, 7.2.0 through 7.2.5, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15 FortiSwitchManager versions 7.2.0 through 7.2.2, 7.0.0 through 7.0.2 allows attacker to execute unauthorized code or commands via specially crafted cli commands and http requests.

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-134: Use of Externally-Controlled Format String

Vulnerability CVE-2023-45586

An insufficient verification of data authenticity vulnerability [CWE-345] in FortiOS & FortiProxy SSL-VPN tunnel mode may allow an authenticated VPN user to send (but not receive) packets spoofing the IP of another user via crafted network packets.

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

Vulnerability CVE-2023-46714

A stack-based buffer overflow [CWE-121] vulnerability in Fortinet FortiOS version 7.2.1 through 7.2.6 and version 7.4.0 through 7.4.1 allows a privileged attacker over the administrative interface to execute arbitrary code or commands via crafted HTTP or HTTPs requests.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/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-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-2023-48784

A use of externally-controlled format string vulnerability [CWE-134] in FortiOS version 7.4.1 and below, version 7.2.7 and below, version 7.0.14 and below, version 6.4.15 and below command line interface may allow a local privileged attacker with super-admin profile and CLI access to execute arbitrary code or commands via specially crafted requests.

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/RC:R
CWE	CWE-134: Use of Externally-Controlled Format String

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-2024-23110

A stack-based buffer overflow in Fortinet FortiOS version 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 all versions allows attacker to execute unauthorized code or commands via specially crafted commands

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/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-2024-23112

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

Vulnerability CVE-2024-23662

An exposure of sensitive information to an unauthorized actor in Fortinet FortiOS at least version at least 7.4.0 through 7.4.1 and 7.2.0 through 7.2.5 and 7.0.0 through 7.0.15 and 6.4.0 through 6.4.15 allows attacker to information disclosure via HTTP requests.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2024-26007

An improper check or handling of exceptional conditions vulnerability [CWE-703] in Fortinet FortiOS version 7.4.1 allows an unauthenticated attacker to provoke a denial of service on the administrative interface via crafted HTTP requests.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-703: Improper Check or Handling of Exceptional Conditions

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 (2024-03-12):	Publication Date
V1.1 (2024-04-09):	Added CVE-2023-42789, CVE-2023-42790, CVE-2023-46717, CVE-2024-23112 and updated remediations
V1.2 (2024-05-14):	Added CVE-2024-23662, CVE-2023-48784, CVE-2023-41677. Adapted title to reflect latest Siemens validated release version of Fortinet NGFW
V1.3 (2024-06-11):	Added newly published upstream CVEs CVE-2023-45586, CVE-2024-26007, CVE-2023-36640, CVE-2023-45583, CVE-2023-44247, CVE-2023-46714
V1.4 (2024-07-09):	Added newly published upstream CVE CVE-2024-23110

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.