SSA-770770: Multiple Vulnerabilities in Fortigate NGFW Before V7.4.7 on RUGGEDCOM APE1808 Devices

Publication Date: 2025-02-11
Last Update: 2025-07-08
Current Version: V1.5
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 9.1

SUMMARY

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

Siemens has released a new version for RUGGEDCOM APE1808 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808:	Update Fortigate NGFW to V7.4.7. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Fortinet NGFW < V7.4.5 affected by CVE-2024-26013, CVE-2024-35279, CVE-2024-36504, CVE-2024-40591, CVE-2024-45324, CVE-2024-46665, CVE-2024-46666, CVE-2024-46668, CVE-2024-46669, CVE-2024-46670, CVE-2024-48884, CVE-2024-48885, CVE-2024-48886, CVE-2024-50563, CVE-2024-50565, CVE-2024-54021	Update Fortigate NGFW to V7.4.7. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Fortinet NGFW < V7.4.7 affected by CVE-2022-42475, CVE-2023-27997, CVE-2024-21762	Update Fortigate NGFW to V7.4.7. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Fortinet NGFW configured to use ASCII authentication < V7.4.7 affected by CVE-2025-22252	Update Fortigate NGFW to V7.4.7. Contact customer support to receive patch and update information See further recommendations from section Workarounds and Mitigations
RUGGEDCOM APE1808: All versions with Fortinet NGFW < V7.4.6 affected by CVE-2024-3596, CVE-2025-22251, CVE-2025-22254	Update Fortigate NGFW to V7.4.7. 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-2022-42475, CVE-2023-27997, CVE-2024-21762: Refer to Fortinet Blog for mitigation measures https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity
- CVE-2024-35279: For each interface, remove the fabric service or block CAPWAP-CONTROL access to port 5246 through a local-in policy (see https://fortiguard.fortinet.com/psirt/FG-IR-24-160)
- CVE-2025-22252: Use alternate authentication mechanism such as PAP, MSCHAP, and CHAP configurations other than ASCII authentication (see https://www.fortiguard.com/psirt/FG-IR-24-472)

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

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-2022-42475

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier and FortiProxy SSL-VPN 7.2.0 through 7.2.1, 7.0.7 and earlier may allow a remote unauthenticated attacker to execute arbitrary 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
CWE	CWE-197: Numeric Truncation Error

Vulnerability CVE-2023-27997

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary 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
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2024-3596

RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify responses Access-Reject or Access-Accept using a chosen-prefix collision attack against MD5 Response Authenticator signature.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v4.0 Base Score	9.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H
CWE	CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel

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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2024-26013

A improper restriction of communication channel to intended endpoints vulnerability [CWE-923] in Fortinet FortiOS version 7.4.0 through 7.4.4, 7.2.0 through 7.2.8, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15 and before 6.2.16, Fortinet FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9 and before 7.0.15, Fortinet FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and before 6.2.13, Fortinet FortiAnalyzer version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and before 6.2.13, Fortinet FortiVoice version 7.0.0 through 7.0.2 before 6.4.8 and Fortinet FortiWeb before 7.4.2 may allow an unauthenticated attacker in a man-in-the-middle position to impersonate the management device (FortiCloud server or/and in certain conditions, FortiManager), via intercepting the FGFM authentication request between the management device and the managed device

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
CWE	CWE-923: Improper Restriction of Communication Channel to Intended Endpoints

Vulnerability CVE-2024-35279

A stack-based buffer overflow vulnerability in Fortinet FortiOS version 7.2.4 through 7.2.8 and version 7.4.0 through 7.4.4 allows a remote unauthenticated attacker to execute arbitrary code or commands via crafted UDP packets through the CAPWAP control, provided the attacker were able to evade FortiOS stack protections and provided the fabric service is running on the exposed interface.

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
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2024-36504

An out-of-bounds read vulnerability [CWE-125] in FortiOS SSLVPN web portal versions 7.4.0 through 7.4.4, versions 7.2.0 through 7.2.8, 7.0 all verisons, and 6.4 all versions may allow an authenticated attacker to perform a denial of service on the SSLVPN web portal via a specially crafted URL.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-40591

An incorrect privilege assignment vulnerability in Fortinet FortiOS version 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.9 and before 7.0.15 allows an authenticated admin whose access profile has the Security Fabric permission to escalate their privileges to super-admin by connecting the targetted FortiGate to a malicious upstream FortiGate they control.

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
CWE	CWE-266: Incorrect Privilege Assignment

Vulnerability CVE-2024-45324

A use of externally-controlled format string vulnerability in FortiOS version 7.4.0 through 7.4.4, version 7.2.0 through 7.2.9, version 7.0.0 through 7.0.15 and before 6.4.15, FortiProxy version 7.4.0 through 7.4.6, version 7.2.0 through 7.2.12 and before 7.0.19, FortiPAM version 1.4.0 through 1.4.2 and before 1.3.1, FortiSRA version 1.4.0 through 1.4.2 and before 1.3.1 and FortiWeb version 7.4.0 through 7.4.5, version 7.2.0 through 7.2.10 and before 7.0.10 allows a privileged attacker to execute unauthorized code or commands via specially crafted HTTP or HTTPS commands.

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
CWE	CWE-134: Use of Externally-Controlled Format String

Vulnerability CVE-2024-46665

An insertion of sensitive information into sent data vulnerability [CWE-201] in FortiOS 7.6.0, 7.4.0 through 7.4.4 may allow an attacker in a man-in-the-middle position to retrieve the RADIUS accounting server shared secret via intercepting accounting-requests.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE	CWE-201: Insertion of Sensitive Information Into Sent Data

Vulnerability CVE-2024-46666

An allocation of resources without limits or throttling [CWE-770] vulnerability in FortiOS versions 7.6.0, versions 7.4.4 through 7.4.0, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow a remote unauthenticated attacker to prevent access to the GUI via specially crafted requests directed at specific endpoints.

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
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2024-46668

An allocation of resources without limits or throttling vulnerability [CWE-770] in FortiOS versions 7.4.0 through 7.4.4, versions 7.2.0 through 7.2.8, versions 7.0.0 through 7.0.15, and versions 6.4.0 through 6.4.15 may allow an unauthenticated remote user to consume all system memory via multiple large file uploads.

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
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2024-46669

An Integer Overflow or Wraparound vulnerability in version 7.4.4 and below, version 7.2.10 and below; FortiSASE version 23.4.b FortiOS tenant IPsec IKE service may allow an authenticated attacker to crash the IPsec tunnel via crafted requests, resulting in potential denial of service.

CVSS v3.1 Base Score	3.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2024-46670

An Out-of-bounds Read vulnerability in FortiOS version 7.6.0, version 7.4.4 and below, version 7.2.9 and below and FortiSASE FortiOS tenant version 24.3.b IPsec IKE service may allow an unauthenticated remote attacker to trigger memory consumption leading to Denial of Service via crafted requests.

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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-48884

A improper limitation of a pathname to a restricted directory (’path traversal’) in Fortinet FortiManager versions 7.6.0 through 7.6.1, 7.4.1 through 7.4.3, FortiOS versions 7.6.0, 7.4.0 through 7.4.4, 7.2.5 through 7.2.9, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15, FortiProxy 7.4.0 through 7.4.5, 7.2.0 through 7.2.11, 7.0.0 through 7.0.18, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiManager Cloud versions 7.4.1 through 7.4.3 allows attacker to trigger an escalation of privilege via specially crafted packets.

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
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory (’Path Traversal’)

Vulnerability CVE-2024-48885

A improper limitation of a pathname to a restricted directory (’path traversal’) in Fortinet FortiRecorder versions 7.2.0 through 7.2.1, 7.0.0 through 7.0.4, FortiWeb versions 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.10, 7.0.0 through 7.0.10, 6.4.0 through 6.4.3, FortiVoice versions 7.0.0 through 7.0.4, 6.4.0 through 6.4.9, 6.0.0 through 6.0.12 allows attacker to escalate privilege via specially crafted packets.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory (’Path Traversal’)

Vulnerability CVE-2024-48886

A weak authentication in Fortinet FortiOS versions 7.4.0 through 7.4.4, 7.2.0 through 7.2.8, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15, FortiProxy versions 7.4.0 through 7.4.4, 7.2.0 through 7.2.10, 7.0.0 through 7.0.17, 2.0.0 through 2.0.14, FortiManager versions 7.6.0 through 7.6.1, 7.4.1 through 7.4.3, FortiManager Cloud versions 7.4.1 through 7.4.3, FortiAnalyzer Cloud versions 7.4.1 through 7.4.3 allows attacker to execute unauthorized code or commands via a brute-force attack.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE	CWE-1390: Weak Authentication

Vulnerability CVE-2024-50563

A weak authentication in Fortinet FortiManager Cloud, FortiAnalyzer versions 7.6.0 through 7.6.1, 7.4.1 through 7.4.3, FortiAnalyzer Cloud versions 7.4.1 through 7.4.3, FortiManager versions 7.6.0 through 7.6.1, 7.4.1 through 7.4.3, FortiManager Cloud versions 7.4.1 through 7.4.3 allows attacker to execute unauthorized code or commands via a brute-force attack.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
CWE	CWE-1390: Weak Authentication

Vulnerability CVE-2024-50565

A improper restriction of communication channel to intended endpoints vulnerability [CWE-923] in Fortinet 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 and 6.2.0 through 6.2.16, Fortinet FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15 and 2.0.0 through 2.0.14, Fortinet FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and 6.2.0 through 6.2.13, Fortinet FortiAnalyzer version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and 6.2.0 through 6.2.13, Fortinet FortiVoice version 7.0.0 through 7.0.2, 6.4.0 through 6.4.8 and 6.0.0 through 6.0.12 and Fortinet FortiWeb version 7.4.0 through 7.4.2, 7.2.0 through 7.2.10, 7.0.0 through 7.0.10 allows an unauthenticated attacker in a man-in-the-middle position to impersonate the management device (FortiCloud server or/and in certain conditions, FortiManager), via intercepting the FGFM authentication request between the management device and the managed device

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
CWE	CWE-300: Channel Accessible by Non-Endpoint

Vulnerability CVE-2024-54021

An improper neutralization of crlf sequences in http headers ('http response splitting') in Fortinet FortiOS 7.2.0 through 7.6.0, FortiProxy 7.2.0 through 7.4.5 allows attacker to execute unauthorized code or commands via crafted HTTP header.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
CWE	CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')

Vulnerability CVE-2025-22251

An improper restriction of communication channel to intended endpoints vulnerability [CWE-923] in FortiOS 7.6.0, 7.4.0 through 7.4.5, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow an unauthenticated attacker to inject unauthorized sessions via crafted FGSP session synchronization packets.

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RC:C
CWE	CWE-923: Improper Restriction of Communication Channel to Intended Endpoints

Vulnerability CVE-2025-22252

A missing authentication for critical function vulnerability in FortiOS, FortiProxy, and FortiSwitchManager TACACS+ configured to use a remote TACACS+ server for authentication, that has itself been configured to use ASCII authentication may allow an attacker with knowledge of an existing admin account to access the device as a valid admin via an authentication bypass.

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
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2025-22254

An Improper Privilege Management vulnerability [CWE-269] affecting Fortinet FortiOS version 7.6.0 through 7.6.1, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10, 7.0.0 through 7.0.16 and before 6.4.15, FortiProxy version 7.6.0 through 7.6.1 and before 7.4.7 & FortiWeb version 7.6.0 through 7.6.1 and before 7.4.6 allows an authenticated attacker with at least read-only admin permissions to gain super-admin privileges via crafted requests to Node.js websocket module.

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:H/RL:W/RC:C
CWE	CWE-269: Improper Privilege Management

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 (2025-02-11):	Publication Date
V1.1 (2025-03-11):	Added newly published upstream vulnerabilities CVE-2024-35279 and CVE-2024-40591
V1.2 (2025-04-08):	Added newly published upstream vulnerabilities CVE-2024-48886, CVE-2024-50563, CVE-2024-45324 and CVE-2024-3596
V1.3 (2025-05-13):	Added newly published upstream vulnerabilities CVE-2024-21762, CVE-2022-42475, CVE-2023-27997, CVE-2024-26013 and CVE-2024-50565. Moved CVE-2024-52963 to SSA-864900
V1.4 (2025-06-10):	Added newly published upstream vulnerability CVE-2025-22252
V1.5 (2025-07-08):	Added newly published upstream vulnerabilities CVE-2025-22254 and CVE-2025-22251

TERMS OF USE