SSA-366067: Multiple Vulnerabilities in Fortigate NGFW before V7.4.1 on RUGGEDCOM APE1808 devices

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

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 before V7.4.1 affected by all CVEs	Update Fortigate NGFW to V7.4.1. 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-2023-25610: Disable HTTP/HTTPS administrative interface OR Limit IP addresses that can reach the administrative interface (see https://www.fortiguard.com/psirt/FG-IR-23-001)
- CVE-2023-27997: Disable SSL-VPN (see https://www.fortiguard.com/psirt/FG-IR-23-097)
- CVE-2023-33308: Disable HTTP/2 support on SSL inspection profiles used by proxy policies or firewall policies with proxy mode (see https://www.fortiguard.com/psirt/FG-IR-23-183)

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-2022-39948

An improper certificate validation vulnerability [CWE-295] in FortiOS 7.2.0 through 7.2.3, 7.0.0 through 7.0.7, 6.4 all versions, 6.2 all versions, 6.0 all versions and FortiProxy 7.0.0 through 7.0.6, 2.0 all versions, 1.2 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the FortiOS/FortiProxy device and remote servers hosting threat feeds (when the latter are configured as Fabric connectors in FortiOS/FortiProxy)

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-2022-41327

A cleartext transmission of sensitive information vulnerability [CWE-319] in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.8, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.8 allows an authenticated attacker with readonly superadmin privileges to intercept traffic in order to obtain other adminstrators cookies via diagnose CLI 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-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2022-41328

A improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in Fortinet FortiOS version 7.2.0 through 7.2.3, 7.0.0 through 7.0.9 and before 6.4.11 allows a privileged attacker to read and write files on the underlying Linux system via 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-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2022-41329

An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.7, FortiOS version 7.2.0 through 7.2.3 and 7.0.0 through 7.0.9 allows an unauthenticated attackers to obtain sensitive logging informations on the device via crafted HTTP GET 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-2022-41330

An improper neutralization of input during web page generation vulnerability ('Cross-site Scripting') [CWE-79] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9, version 6.4.0 through 6.4.11 and before 6.2.12 and FortiProxy version 7.2.0 through 7.2.1 and before 7.0.7 allows an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests.

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-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2022-41334

An improper neutralization of input during web page generation [CWE-79] vulnerability in FortiOS versions 7.0.0 to 7.0.7 and 7.2.0 to 7.2.3 may allow a remote, unauthenticated attacker to launch a cross site scripting (XSS) attack via the "redir" parameter of the URL seen when the "Sign in with FortiCloud" button is clicked.

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-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2022-42469

A permissive list of allowed inputs vulnerability [CWE-183] in FortiGate version 7.2.3 and below, version 7.0.9 and below Policy-based NGFW Mode may allow an authenticated SSL-VPN user to bypass the policy via bookmarks in the web portal.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-183: Permissive List of Allowed Inputs

Vulnerability CVE-2022-42474

A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before 6.4.12, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.7, FortiSwitchManager version 7.2.0 through 7.2.1 and before 7.0.1 allows an privileged attacker to delete arbitrary directories from the filesystem through crafted HTTP requests.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-23: Relative Path Traversal

Vulnerability CVE-2022-42476

A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.11, FortiProxy version 7.2.0 through 7.2.2 and 7.0.0 through 7.0.8 allows privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-23: Relative Path Traversal

Vulnerability CVE-2022-43947

An improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiOS version 7.2.0 through 7.2.3 and before 7.0.10, FortiProxy version 7.2.0 through 7.2.2 and before 7.0.8 administrative interface allows an attacker with a valid user account to perform brute-force attacks on other user accounts via injecting valid login sessions.

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-307: Improper Restriction of Excessive Authentication Attempts

Vulnerability CVE-2022-43953

A use of externally-controlled format string in Fortinet FortiOS version 7.2.0 through 7.2.4, FortiOS all versions 7.0, FortiOS all versions 6.4, FortiOS all versions 6.2, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7 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-2022-45861

An access of uninitialized pointer vulnerability [CWE-824] in the SSL VPN portal of Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before 6.4.11 and FortiProxy version 7.2.0 through 7.2.1, version 7.0.0 through 7.0.7 and before 2.0.11 allows a remote authenticated attacker to crash the sslvpn daemon via an HTTP GET request.

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/E:P/RL:O/RC:C
CWE	CWE-824: Access of Uninitialized Pointer

Vulnerability CVE-2023-22639

A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows attacker to escalation of privilege via specifically 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-787: Out-of-bounds Write

Vulnerability CVE-2023-22640

A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.

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-787: Out-of-bounds Write

Vulnerability CVE-2023-22641

A url redirection to untrusted site ('open redirect') in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.9, FortiOS versions 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specially crafted requests.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

Vulnerability CVE-2023-25610

A buffer underwrite ('buffer underflow') vulnerability in FortiOS, FortiManager, FortiAnalyzer, FortiWeb, FortiProxy & FortiSwitchManager administrative interface may allow a remote unauthenticated attacker to execute arbitrary code on the device and/or perform a DoS on the GUI, 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-20: Improper Input Validation

Vulnerability CVE-2023-26207

An insertion of sensitive information into log file vulnerability in Fortinet FortiOS 7.2.0 through 7.2.4 and FortiProxy 7.0.0 through 7.0.10. 7.2.0 through 7.2.1 allows an attacker to read certain passwords in plain text.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-532: Insertion of Sensitive Information into Log File

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/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-28001

An insufficient session expiration in Fortinet FortiOS 7.0.0 - 7.0.12 and 7.2.0 - 7.2.4 allows an attacker to execute unauthorized code or commands via reusing the session of a deleted user in the REST API.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-613: Insufficient Session Expiration

Vulnerability CVE-2023-28002

An improper validation of integrity check value vulnerability [CWE-354] in FortiOS VMs may allow a local attacker with admin privileges to boot a malicious image on the device and bypass the filesystem integrity check in place.

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-354: Improper Validation of Integrity Check Value

Vulnerability CVE-2023-29175

An improper certificate validation vulnerability [CWE-295] in FortiOS 6.2 all versions, 6.4 all versions, 7.0.0 through 7.0.10, 7.2.0 and FortiProxy 1.2 all versions, 2.0 all versions, 7.0.0 through 7.0.9, 7.2.0 through 7.2.3 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the vulnerable device and the remote FortiGuard's map server.

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-2023-29178

A access of uninitialized pointer vulnerability [CWE-824] in Fortinet FortiProxy version 7.2.0 through 7.2.3 and before 7.0.9 and FortiOS version 7.2.0 through 7.2.4 and before 7.0.11 allows an authenticated attacker to repetitively crash the httpsd process via crafted HTTP or HTTPS requests.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-824: Access of Uninitialized Pointer

Vulnerability CVE-2023-29179

A NULL pointer dereference vulnerability [CWE-476] in FortiOS may allow an authenticated attacker to crash the SSL-VPN daemon via specially crafted HTTP requests to the /proxy endpoint

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/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-29180

A NULL pointer dereference vulnerability [CWE-476] in FortiOS may allow a remote unauthenticated attacker to crash the SSL-VPN daemon via specially crafted HTTP 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/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-29181

A use of externally-controlled format string vulnerability [CWE-134] in the Fclicense daemon of FortiOS may allow a remote authenticated attacker to execute arbitrary code or commands via specially crafted 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-20: Improper Input Validation

Vulnerability CVE-2023-29183

An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 and FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14 GUI may allow an authenticated attacker to trigger malicious JavaScript code execution via crafted guest management setting.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/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-2023-33301

An improper access control vulnerability in Fortinet FortiOS 7.2.0 - 7.2.4 and 7.4.0 allows an attacker to access a restricted resource from a non trusted host.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2023-33305

A loop with unreachable exit condition ('infinite loop') in Fortinet FortiOS version 7.2.0 through 7.2.4, FortiOS version 7.0.0 through 7.0.10, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0 all versions, FortiProxy version 7.2.0 through 7.2.3, FortiProxy version 7.0.0 through 7.0.9, FortiProxy 2.0 all versions, FortiProxy 1.2 all versions, FortiProxy 1.1 all versions, FortiProxy 1.0 all versions, FortiWeb version 7.2.0 through 7.2.1, FortiWeb version 7.0.0 through 7.0.6, FortiWeb 6.4 all versions, FortiWeb 6.3 all versions allows attacker to perform a denial of service via specially crafted HTTP requests.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability CVE-2023-33306

A NULL pointer dereference vulnerability [CWE-476] in SSL-VPN may allow an authenticated remote attacker to trigger a crash of the SSL-VPN service via crafted requests.

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/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2023-33307

A NULL pointer dereference vulnerability [CWE-476] in SSL-VPN may allow an authenticated remote attacker to trigger a crash of the SSL-VPN service via crafted requests.

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/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2023-33308

A stack-based overflow vulnerability [CWE-124] in Fortinet FortiOS version 7.0.0 through 7.0.10 and 7.2.0 through 7.2.3 and FortiProxy version 7.0.0 through 7.0.9 and 7.2.0 through 7.2.2 allows a remote unauthenticated attacker to execute arbitrary code or command via crafted packets reaching proxy policies or firewall policies with proxy mode alongside deep or full packet inspection.

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2023-36555

An improper neutralization of script-related html tags in a web page (basic xss) in Fortinet FortiOS 7.2.0 - 7.2.4 allows an attacker to execute unauthorized code or commands via the SAML and Security Fabric components.

CVSS v3.1 Base Score	3.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2023-36639

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, FortiOS versions 7.4.0, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiPAM versions 1.0.0 through 1.0.3 allows attacker to execute unauthorized code or commands via specially crafted API 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-134: Use of Externally-Controlled Format String

Vulnerability CVE-2023-36641

A null pointer dereference [CWE-476] in FortiOS and FortiProxy SSL VPN may allow an authenticated attacker to perform a DoS attack on the device via specifically crafted HTTP requests.

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/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2023-37935

A use of GET request method with sensitive query strings vulnerability in Fortinet FortiOS 7.0.0 - 7.0.12, 7.2.0 - 7.2.5 and 7.4.0 allows an attacker to view plaintext passwords of remote services such as RDP or VNC, if the attacker is able to read the GET requests to those services.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-598: Use of GET Request Method With Sensitive Query Strings

Vulnerability CVE-2023-40718

A interpretation conflict in Fortinet IPS Engine versions 7.321, 7.166 and 6.158 allows attacker to evade IPS features via crafted TCP 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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-436: Interpretation Conflict

Vulnerability CVE-2023-41675

A use after free vulnerability [CWE-416] in FortiOS version 7.2.0 through 7.2.4 and version 7.0.0 through 7.0.10 and FortiProxy version 7.2.0 through 7.2.2 and version 7.0.0 through 7.0.8 may allow an unauthenticated remote attacker to crash the WAD process via multiple crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection.

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-416: Use After Free

Vulnerability CVE-2023-41841

An improper authorization vulnerability in Fortinet FortiOS 7.0.0 - 7.0.11 and 7.2.0 - 7.2.4 allows an attacker belonging to the prof-admin profile to perform elevated actions.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-285: Improper Authorization

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

TERMS OF USE