Multiple Vulnerabilities in FortiOS v7.2.4 and Earlier

Overview

Several vulnerabilities impacting FortiOS version 7.2.4 and earlier were recently published, with individual CVEs listed below under the Vulnerability Details section. GE Gas Power has identified several of its own products that include an impacted FortiOS version, listed below under Affected Products and Versions.

Affected Products and Versions

GE Products:

- NetworkST4 (301E or 401E)
- Remote Operations Offering (101F)
- M&D Lockbox (60F)

FortiOS Versions:

- FortiOS version 7.2.4 and below

Vulnerability Details

A list of vulnerabilities impacting FortiOS versions 7.2.4 and below is provided in the table below.

CVE ID	CVSSv3	Impacted Versions	Description
CVE-2023-27997	9.8	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.11 FortiOS 6.4.0 – 6.4.12 FortiOS 6.0.0 – 6.0.16	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS impacting all versions of SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.
CVE-2023-28001	9.8	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.12	An insufficient session expiration in Fortinet FortiOS allows an attacker to execute unauthorized code or commands by reusing the session of a deleted user in the REST API.
CVE-2023-29178	4.3	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.2.10	An access of uninitialized pointer vulnerability [CWE-824] in FortiOS allows an authenticated attacker to repetitively crash the httpsd process via crafted HTTP or HTTPS requests.
CVE-2023-29183	8.0	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.11 FortiOS 6.4.0 – 6.4.12 FortiOS 6.2.0 – 6.2.14	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiOS GUI may allow an authenticated attacker to trigger malicious JavaScript code execution via crafted guest management settings.

CVE-2023-33305	6.5	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.10 FortiOS 6.x	A loop with unreachable exit condition ('infinite loop') in FortiOS allows an attacker to perform a denial-of-service attack via specially crafted HTTP requests.
CVE-2023-33306	6.5	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.11 FortOS 6.4.0 – 6.4.12	A null pointer dereference in Fortinet FortiOS allows an attacker to perform a denial of SSL-VPN service attack via a specifically crafted request in bookmark parameters.
CVE-2023-41675	4.8	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.10	A use after free vulnerability [CWE-416] in FortiOS may allow an unauthenticated remote attacker to crash the Web Proxy process via multiple crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection.
CVE-2023-41841	7.4	FortiOS 7.2.0 – 7.2.4 FortiOS 7.0.0 – 7.0.11	An improper authorization vulnerability [CWE-285] in FortiOS's WEB UI component may allow an authenticated attacker belonging to the prof-admin profile to perform elevated actions.

Exploitation Status

GE Gas Power Product Security has not yet observed nor received reports of any exploit attempts against Gas Power Customers.

Remediation/Mitigation

For customers with an M&D Lockbox, FortiOS version 7.4.1 has been validated. The Lockbox should be updated to FortiOS v7.4.1 to mitigate each of the vulnerabilities listed above.

For customers with either NetworkST4 or the Remote Operations Offering, GE Gas Power has completed validating FortiOS v7.2.5 to ensure that existing configurations will continue to work when updated. If you have either of these devices, they should be updated to FortiOS v7.2.5.

If you have any questions or issues updating to either new version of FortiOS, please reach out to your local GE Services representative for assistance.

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	10/19/2023	Initial Release