FortiOS and FortiProxy Multiple Vulnerabilities

Overview

Several FortiOS and FortiProxy vulnerabilities were published on February 8th, 2024, under the IDs CVE-2024-23113, CVE-2024-21762, CVE-2023-47537, and CVE-2023-44487. GE Vernova has identified several of its products that include an impacted FortiOS version, listed below.

Affected Products and Versions

GE Vernova Products:

- NetworkST4 (301E or 401E)
- Remote Operations Offering (101E or 101F)
- S3C Firewall (60F)
- M&D Lockbox (60F)

Impacted FortiOS Versions:

Version	Affected
FortiOS 7.4	7.2.0 through 7.4.2
FortiOS 7.2	7.2.0 through 7.2.6
FortiOS 7.0	7.0.0 through 7.0.13
FortiOS 6.4	6.4.0 through 6.4.14
FortiOS 6.2	6.2.0 through 6.2.15
FortiOS 6.0	6.0 all versions

Vulnerability Details – Format String Bug in fgfmd

CVSSv3 Score: 9.8 (Critical)

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.

https://www.fortiguard.com/psirt/FG-IR-24-029

Vulnerability Details – Out-of-bounds write in sslvpnd

CVSSv3 Score: 9.6 (Critical)

An out-of-bounds write vulnerability [CWE-787] in FortiOS and FortiProxy may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

GE Vernova has recommended in a previous advisory to disable SSL-VPN functionality as it is not used with Gas Power installations.

https://www.fortiguard.com/psirt/FG-IR-24-015

Vulnerability Details – Fortilink lack of certificate validation

CVSSv3 Score: 4.4 (Medium)

An improper certificate validation vulnerability [CWE-295] in FortiOS may allow an unauthenticated attacker in a Man-in-the-Middle position to decipher and alter the FortiLink communication channel between the FortiOS device and a FortiSwitch instance.

https://www.fortiguard.com/psirt/FG-IR-23-301

Vulnerability Details – Rapid Reset HTTP/2 vulnerability

CVSSv3 Score: 5.3 (Medium)
The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly.
https://www.fortiguard.com/psirt/FG-IR-23-397

Exploitation Status

GE Vernova has not yet observed nor received reports of any compromise of Gas Power customer equipment due to these vulnerabilities.

Remediation/Mitigation

The S3C Firewall and Lockbox devices (FortiGate 60F) provided by GE Gas Power M&D should be updated to FortiOS version 7.4.3.

NetworkST4 devices (FortiGate 301E and 401E) as well as the Remote Operations Offering (FortiGate 101E and 101F) should be updated to FortiOS version 7.2.7.

If you need support in updating any of the products mentioned above to the appropriate version of FortiOS for your equipment, 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	3/5/2024	Initial Release