GE Vernova
Steam Power
Nuclear P&L

March 26, 2024 **CYBERSECURITY**

Topic: FortiOS Multiple Vulnerabilities

Overview

In February 2024, critical vulnerabilities are published in FortiOS known as CVE-2024-23113, CVE-2024-21762, CVE-2023-42789, CVE-2023-42790.

GE Vernova Steam Power Nuclear P&L has identified several of its products that include an impacted FortiOS version, listed below.

Affected Products and Versions

- Alspa Remote Access (FG60D,E,F,G or FG100D, E ,F, G)
- Mark Vie Network ST4.0 (FG301E or FG401E)
- All GE Steam Power solutions using Fortigate solution
  - FortiGate FG100 D, E, F.
  - FortiGate FG60 D, E, F.

Impacted FortiOS versions

- FortiOS versions 7.4. before 7.4.3
- FortiOS versions 7.2.x before 7.2.7
- FortiOS versions 7.0.x before 7.0.14
- FortiOS versions 6.4.x before 6.4.15
- FortiOS versions 6.2.x before 6.2.16
- FortiOS 6.0 all versions

CVE-2024-2313 - 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
https://www.fortiguard.com/psirt/FG-IR-24-029

CVE-2024-21762 - 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.
https://www.fortiguard.com/psirt/FG-IR-24-015

CVE-2023-42789, CVE-2023-42790 Out-of-bounds Write in captive porta

An out-of-bounds write vulnerability [CWE-787] and a Stack-based Buffer Overflow [CWE-121] in FortiOS & FortiProxy captive portal may allow an inside attacker who has

access to captive portal to execute arbitrary code or commands via specially crafted HTTP requests.
https://www.fortiguard.com/psirt/FG-IR-23-328

Urgent containment
While the vulnerability is not fixed with an update, GE Vernova Steam Power Nuclear P&L strongly recommends to disable SSL VPN on Fortigate (disable webmode is NOT a valid workaround)

For Network ST4.0, GE Vernova recommends disabling permanently SSL-VPN functionality as it is not used.
For Alspa Remote Access with Forticlient, VPN – SSL should be stopped, Firewall disconnected from internet. The function is not available anymore until the problem is fixed.

CVE-2024-2313 Workaround
FortiOS 6.x is not affected.
For each interface, remove the fgfm access. Refer to following article for details
https://www.fortiguard.com/psirt/FG-IR-24-029

CVE-2023-42789, CVE-2023-42790 Workaround
Refer to the following article : https://www.fortiguard.com/psirt/FG-IR-23-328

Exploitation Status
GE Vernova has not yet observed nor received reports of any compromise of Nuclear P&L customer equipment due to these vulnerabilities.

Remediation / Mitigation

For Mark Vie NetworkST4 devices (FortiGate 301E and 401E) should be updated to FortiOS version 7.2.7.

For Alspa Remote Access, Fortigate 60E, 60F and 60G, Fortigate 100E, 100F and 100G, firmware should be updated according to following rules:

Version	Affected	Solution
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above

FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0.0 through 6.0.17	Upgrade to 6.0.18 or above

For Alspa Remote Access with Fortigate 60D and Fortigate 100D, as already communicated, Last Service Extension date from Fortinet was in 2022. Our recommendation is to upgrade the current Firewall product with new firewall solution still in active life.

we recommend to follow the FortiGate PSIRT Advisories: FG-IR-23-097

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 Vernova Steam Power Nuclear P&L representative for assistance.

Reminder
it is mandatory, as a security rule, to keep the FortiGate fully operational from security perspective and to respect following practises

- Firmware & General Updates Support contracts should be subscribed
- Firmware should be updated regularly.

Defense-in-depth
To minimize the risk of the exploitation of current and future system vulnerabilities, GE Steam Power highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your GE Power Automation & Controls salesperson or our Help Desk at +33 1 60 13 43 91 / helpdesk.control-systems@ge.com for help with ordering cybersecurity services and solutions.

Revision History

Version	Release Date	Purpose
A	March 26, 2024	Initial version