june 28, 2023   **CYBERSECURITY**

Topic: FortiOS SSL-VPN Buffer Overflow | CVE-2023-27997

Fortinet published a FortIOS vulnerability alert on June 12, 2023, under the ID CVE-2023-27997 reference.
It describes a heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN
Here the Fortinet recommendation for this vulnerability: CVE-2023-27997 advisory

For Mark Vie products family, GE GAS Power identified that this vulnerability impacts following GE component

- : • NetworkST4 (301E or 401E).

We invite our customer impacted by this alert to consult GE recommendation on following link : FortiOS SSL-VPN Buffer Overflow | CVE-2022-42475 / CVE-2023-27997

For other GE STEAM Power products using FortiGate solution like:

- FortiGate FG100 D, E, F with SSL portal function.
- FortiGate FG60 D, E, F with SSL portal function.

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

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	June 28, 2023	Initial version