GE
Steam Power
Automation & Controls

February 017, 2023 **CYBERSECURITY**

Topic: FortiOS SSL-VPN Buffer Overflow | CVE-2022-42475

Dear Valued Customer,

Fortinet published a FortIOS vulnerability on December 12, 2022 under the ID CVE-2022-42475.
It describes a heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN

GE has identified that this vulnerability impact a component of our Mark VIe family

- GE Products: • 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

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.

Specifically, for this point GE recommends users take these defensive measures to minimize the risk of exploitation of this vulnerability:

- Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from outside of the Control System.
- Follow good network design practices, such as implementing network segmentation, and use DMZs with properly configured firewalls to selectively control, and monitor all traffic passed between zones and systems.
- Monitor and log all network traffic attempting to reach affected products for suspicious activity.
- Close all unused ports on affected systems.
- Restrict system access to authorized personnel only and follow a least privilege approach.
- Perform access control checks to limit which users can access the feature that requires the hard-coded credentials. For example, a feature might only be enabled through the system console instead of through a network connection.

© General Electric and/or its affiliates 2022. This Bulletin has been prepared by GE Steam Power Inc. ("GE") for its customers ("Customer") to inform about a vulnerability in an equipment. GE specifically disclaims any responsibility for liability for damage of any type, i.e., direct, consequential, or special that may be alleged to have been incurred as result of applying this information. This Bulletin does not vary any contractual relationship between GE and the Customer as the case maybe. This document contains proprietary and confidential information of GE and shall not be reproduced, nor shall its contents be disclosed to any third party or used for different purposes without the written approval of GE management.

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.

Hugues Moreau
Product Manager Power Automation & Controls, GE Steam Power
Hugues.moreau@ge.com

Revision History

Version	Release Date	Purpose
A	February 17, 2023	Initial version