

Vulnerability In FortiOS | CVE-2022-41328

Overview

GE Gas Power has been made aware of a vulnerability in FortiOS that became public information on March 7th, 2023. [CVE-2022-41328](#) has been assigned to this vulnerability.

Vulnerability Details

A improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in FortiOS may allow a privileged attacker to read and write arbitrary files via crafted CLI commands.

Affected Products and Versions

GE Products:

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

FortiOS Versions:

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.9
- FortiOS version 6.4.0 through 6.4.11
- FortiOS version 6.2.0 all versions
- FortiOS 6.0 all versions

Severity Assessment

While the vendor has classified this vulnerability as Medium, GE Gas Power has determined the actual risk to our customers to be low due to other existing controls to prevent access to administrative interface outside of plant networks.

Exploitation Status

GE Gas Power Product Security is not aware of any malicious attempts to exploit this vulnerability in customer equipment.

Remediation

FortiGuard has released a firmware update (FortiOS 7.2.4) to address this vulnerability across their line of products and recommends updating device firmware to this version to resolve this issue. Further details on affected and recommended versions can be found in the advisory from the vendor:

<https://www.fortiguard.com/psirt/FG-IR-22-369>

GE Gas Power M&D has validated the new firmware against S3C and Lockbox configurations of the 60F and will begin rolling out the update directly to M&D customers. If you own a 60F device as part of a LockBox or S3C firewall configuration, no action is required on your part at this time.

GE Gas Power Engineering has validated the new firmware against NetworkST 4.0 equipment (301E and 401E) and the Remote Operations Offering (101F) configuration. If your site has an active support contact with Fortinet, download the newer firmware from Fortinet and apply the update to the

equipment. The Fortinet [upgrade path](#), available in the FortiGate portal, should be used while upgrading from older revisions of firmware to higher versions.

Reach out to your local GE Services representative for any support with upgrade path to be followed and any issues observed post firmware upgrade.

Additionally, if you have already performed an upgrade to FortiOS v7.2.4 in response to the [previous FortiOS advisory regarding a buffer underflow issue](#), no action is required on your part at this time.

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are engineered with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers.

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	April 6 th , 2023	Initial release
2.0	April 25 th , 2023	Updated information on upgrade path