Vulnerability In FortiOS | CVE-2022-40684

Overview

GE Gas Power has been made aware of a vulnerability in FortiOS that became public information on October 10th, 2022. CVE-2022-40684 has been assigned to this vulnerability.

Vulnerability Details

CVE-2022-40684

The vulnerability allows bypassing authentication by sending specially crafted HTTP or HTTPS requests via the administrative interface.

Affected Products and Versions

Fortigate 60F (as could be used in M&D Lockbox Configurations)
FortiOS versions 7.0.0-7.0.6 and 7.2.0-7.2.1

Severity Assessment:

While the vendor has classified this vulnerability as critical, 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. Fortinet has had reports of exploited equipment in the field, and recommends looking for the following indicators of compromise (IOC) in the device's log file:

```
user=”Local_Process_Access”

# show system admin
edit "fortigate-tech-support"
set accprofile "super_admin"
set vdom "root"
set password ENC [...]
next
```

Remediation / Fixes

FortiGuard has released a firmware update (FortiOS 7.2.3) 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-22-377

GE Gas Power M&D is currently investigating impacted devices and our ability to perform the firmware update directly on behalf of our customers. 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	December 14, 2022	Initial release
2.0	December 16, 2022	Updated indicators of compromise and impacted versions list