FortiOS Stack-Based Buffer Overflow | CVE-2023-33308

Overview

A FortiOS vulnerability was published on July 11th, 2023 under the ID CVE-2023-33308. It describes a stack-based buffer overflow vulnerability [CWE-124] in FortiOS. GE Gas Power has identified several of its own products that include an impacted FortiOS version, listed below.

Affected Products and Versions

GE Products:

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

FortiOS Versions:

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.10
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.9

Vulnerability Details

The vulnerability impacts FortiOS by allowing a remote attacker to execute arbitrary code or commands via crafted packets reaching proxy or firewall policies.

Exploitation Status

GE Gas Power Product Security has not yet observed nor received reports of any exploit attempts against Gas Power Customers.

Remediation/Mitigation

Impacted products should be updated to FortiOS version 7.2.4. As part of several previous security advisories released by GE Gas Power pertaining to Fortigate devices, we have already recommended an update to v7.2.4. If you have already updated your equipment in accordance with these previous advisories, no action is required on your part.

If you have not updated any of the impacted products listed above to FortiOS v7.2.4, please reach out to your local GE Services representative for assistance.
https://www.fortiguard.com/psirt/FG-IR-23-183

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	7/25/2023	Initial Release