FortiOS – Multiple Vulnerabilities

Overview

In November 2024 and March 2025, Fortinet published several advisories detailing vulnerabilities impacting FortiOS, including improper authentication, text injection, session hijacking, and string format issues. This advisory references Fortinet's security advisory articles FG-IR-24-325, FG-IR-23-475, FG-IR-24-032, and FG-IR-24-033.

Affected Products and Versions

FortiOS < 7.2.10

- NetworkST4 (FortiGate 301E and 401E)
- Remote Operations Offering (FortiGate 101E and 101F)

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2025-45324	7.0 (High)	6.1 (Medium)	FortiOS	Execute Unauthorized Code (CWE-134)
CVE-2023-50176	7.1 (High)	6.0 (Medium)	FortiOS	Execute Unauthorized Code (CWE-384)
CVE-2024-26011	5.2 (Medium)	2.0 (Low)	FortiOS	Execute Unauthorized Code (CWE-306)
CVE-2024-33510	3.6 (Low)	1.8 (Low)	FortiOS	Improper Access Control (CWE-358)

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

Exploitation Status

GE Vernova has not observed nor received reports of any compromise of Gas Power customer equipment due to this vulnerability.

Remediation/Mitigation

NetworkST4 devices (FortiGate 301E and 401E) as well as the Remote Operations Offering (FortiGate 101E and 101F) should be updated to FortiOS version 7.2.10.

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information.
For Product Security issues or incident/vulnerability reporting: https://www.gevernova.com/security

Document History

Version	Release Date	Purpose
1.0	4/15/2025	Initial Release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.