FortiOS: CVE-2024-52965, CVE-2025-24477, CVE-2024-55599

Overview

In July 2025, Fortinet published three vulnerabilities (CVE-2024-52965, CVE-2025-24477, and CVE-2024-55599) impacting FortiOS.

Affected Products and Versions

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

FortiOS 7.6.2 and below
FortiOS 7.4.7 and below
FortiOS 7.2.11 and below
FortiOS 7.0.17 and below

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2024-52965	6.8 (Medium)	6.0 (Medium)	FortiOS	Improper Access Control (CWE-304)
CVE-2025-24477	4.0 (Medium)	3.3 (Low)	FortiOS	Escalation of Privilege (CWE-122)
CVE-2024-55599	4.9 (Medium)	2.9 (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.

For Gas Power Controls customers, the vulnerabilities listed above impact FortiGate 301E and 401E switches used in NetworkST4, as well as the 101E and 101F used in the Remote Operations Offering.

These vulnerabilities could allow authentication with an invalid certificate, elevation of privileges due to a buffer overflow, or bypass of the DNS filter using Apple devices.

Exploitation Status

GE Vernova has not yet observed or received any reports that Gas Power customer equipment has been compromised due to these vulnerabilities.

Remediation/Mitigation (Gas Power Customers)

For Gas Power Controls customers, FortiOS version 7.4.8 has been validated and approved for installation to address these vulnerabilities.

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	11/11/2025	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 customers. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.