CVE-2025-61624 – Fortinet FortiOS, FortiProxy, FortiPAM Path Traversal Vulnerability Allows File Write and Deletion

TL;DR

CVE-2025-61624 (CVSS not provided) is a path traversal vulnerability affecting Fortinet FortiOS, FortiPAM, FortiProxy, and FortiSwitchManager.

A privileged attacker can write or delete files using crafted CLI commands. Organizations should upgrade immediately to prevent system manipulation.

Overview

CVE-2025-61624 (CVSS not provided) is a path traversal vulnerability in the command line interface (CLI) of multiple Fortinet products, including FortiOS, FortiPAM, FortiProxy, and FortiSwitchManager.

Affected Products

- FortiOS – 6.4, 7.0, 7.2 (all versions), 7.4.0–7.4.9, 7.6.0–7.6.4
- FortiPAM – 1.0–1.6 (all versions), 1.7.0
- FortiProxy – 7.0, 7.2 (all versions), 7.4.0–7.4.11, 7.6.0–7.6.4
- FortiSwitchManager – 7.0.0–7.0.6, 7.2.0–7.2.7

The vulnerability allows a privileged attacker to bypass directory restrictions and execute file write or delete actions by passing crafted arguments to existing CLI commands. This can impact system files, configurations, and logs.

This issue requires authenticated, privileged access. However, once a threat actor gains access (via stolen credentials or another vulnerability), this becomes a reliable way to manipulate systems or disrupt operations. Organizations should treat this as a serious post access issue and upgrade affected systems. Aspire recommends patching as soon as possible to prevent disruption or unauthorized changes.

Aspire Protects

- **Patch** – Upgrade to fixed versions immediately. See Fortinet's advisory for more information.
- Restrict CLI access to authorized administrators only.
- Monitor CLI command activity for unusual behavior.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit this vulnerability after gaining privileged access to modify or delete system files

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using Fortinet FortiOS, FortiProxy, FortiPAM, or FortiSwitchManager are at risk.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

PSIRT | FortiGuard Labs