New FortiWeb Zero-Day Gives Attackers Code Execution on Firewalls

TL;DR

A new FortiWeb zero-day, tracked as CVE-2025-58034, is being actively exploited and allows authenticated attackers to run unauthorized code on FortiWeb Web Application Firewalls. This vulnerability follows last week's FortiWeb zero-day (CVE-2025-64446) where attackers created admin-level accounts on exposed devices.

Fortinet has now confirmed exploitation in the wild and issued patches. Organizations running FortiWeb should upgrade immediately and check for signs of compromise.

Overview

Fortinet released an advisory today for a FortiWeb zero-day vulnerability tracked as CVE-2025-58034, CVSS 6.7. The flaw allows authenticated attackers to trigger OS command injection using crafted HTTP requests or CLI commands.

Once triggered, the attacker is able to run unauthorized code directly on the underlying system. Trend Micro researchers have already observed roughly 2,000 detections in active attacks, confirming exploitation.

CVE-2025-58034 stems from improper sanitization of special characters in commands passed through FortiWeb. When an authenticated user sends a crafted HTTP request or CLI input, the device processes those characters as OS-level commands instead of treating them as text. **This opens the door for an attacker to run arbitrary commands on the firewall.**

This vulnerability impacts multiple versions of FortiWeb across active customer deployments, including:

- FortiWeb 8.0.0 – 8.0.1 - Upgrade to 8.0.2+
- FortiWeb 7.6.0 – 7.6.5 - Upgrade to 7.6.6+
- FortiWeb 7.4.0 – 7.4.10 - Upgrade to 7.4.11+
- FortiWeb 7.2.0 – 7.2.11 - Upgrade to 7.2.12+
- FortiWeb 7.0.0 – 7.0.11 - Upgrade to 7.0.12+

This vulnerability comes right after last week's FortiWeb vulnerability (CVE-2025-64446), where attackers abused a path confusion flaw to create new administrator accounts on internet-facing devices.

Fortinet patched CVE-2025-58034 and CISA has already it to its Known Exploited Vulnerabilities catalog. Federal agencies have until November 25, 2025, to patch. Aspire recommends patching this vulnerability as soon as possible.

Aspire Protects

- **Patch** – Organizations should patch immediately. Please see Fortinet's advisory for further details.
- Review logs for suspicious or unexpected administrative actions, unusual CLI activity, or crafted HTTP requests.
- Check for unauthorized accounts
- Restrict management access to trusted networks only; authenticate with MFA.
- Ensure FortiWeb devices are not internet-facing unless absolutely required.

TTPs to Watch

Execution

- Command and Scripting Interpreter [T1059] – The attacker may have executed system-level commands through crafted HTTP requests or CLI inputs after exploiting the command injection flaw.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may have used the injected commands to gain higher access on the device.

Persistence

- Create Account [T1136] – Even though this vulnerability focuses on command execution, attackers have recently used FortiWeb weaknesses to create unauthorized admin accounts. It remains a key behavior defenders should check for during investigations.

IoCs

Behavioral IoCs to look for:

- Unusual or malformed HTTP requests targeting administrative or API paths
- Unexpected CLI commands executed at odd hours or outside maintenance windows
- Any signs of new or modified user accounts
- Logs showing repeated authentication attempts followed by command execution
- Configuration changes made without a corresponding change ticket
- Unexpected restarts or system messages indicating service interruption
- Signs of traffic routed through unknown proxy or callback infrastructure

Targeted Industries

This FortiWeb firewall zero-day threatens any organization using Fortinet appliances for perimeter security or web application protection:

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's 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

NVD - CVE-2025-58034