Active Fortinet Heap Overflow Flaw Allows Remote Code Execution

TL;DR

Fortinet issued an advisory for a heap-based buffer overflow in FortiOS and FortiSwitchManager that allows unauthenticated remote code execution.

*The issue is in the **cw_acd daemon** and affects a wide range of versions and requires patching. There is no new CVE because this activity is already tracked under existing identifier(s).*

Overview

Fortinet published an advisory for a heap-based buffer overflow (CWE-122, CVSS 7.4) in the ***cw_acd daemon*** affecting multiple FortiOS and FortiSwitchManager versions. The flaw can be triggered remotely without authentication by sending specially crafted network requests to exposed services, allowing an attacker to execute arbitrary code or system commands.

Affected Products

- FortiOS – versions 6.4.0 through 7.6.3
- FortiSwitchManager – versions 7.0.0 through 7.2.6
- FortiSASE – select 25.x releases

These products usually sit at the edge of the network, and while the attack isn't easy to pull off, the access it provides can let an attacker interfere with traffic, move deeper into the environment, or maintain a foothold depending on how the device is being used. This vulnerability affects FortiOS and FortiSwitchManager systems that handle network traffic. If exploited, an attacker gains a trusted position inside the environment, not just access to a single system. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – Patch immediately to the fixed versions published by Fortinet. Find the Upgrade Path Tool here.
- If patching is delayed, restrict or remove fabric access on exposed interfaces.
- Block CAPWAP-CONTROL traffic (UDP 5246–5249) where not required.
- Review external exposure of Fortinet management services.
- Monitor for unusual traffic patterns targeting Fortinet infrastructure.

TTPs

Initial Access

- Exploit Public-Facing Application [T1190] –The attacker may exploit a heap-based buffer overflow in the ***cw_acd daemon*** by sending crafted requests to exposed FortiOS or FortiSwitchManager services, allowing unauthenticated remote access.

Execution

- Command and Scripting Interpreter [T1059] – Once exploitation succeeds, the attacker may execute arbitrary system commands in the context of the affected service account on the device.

Persistence

- Create or Modify System Process [T1543] (conditional) – If the attacker chooses to maintain access, they may modify or create system-level processes or services on the affected Fortinet device, depending on privileges and configuration.

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

This FortiOS and FortiSwitchManager remote code execution vulnerability threatens any organization using Fortinet infrastructure at the network perimeter.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance

- Technology
- Legal
- 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
PSIRT | FortiGuard Labs
PSIRT | FortiGuard Labs
PSIRT | FortiGuard Labs
PSIRT | FortiGuard Labs
PSIRT | FortiGuard Labs
CVE Record: CVE-2025-25249
CVE Record: CVE-2025-64155
CVE Record: CVE-2025-58693
CVE Record: CVE-2025-59922
CVE Record: CVE-2025-67685
CVE Record: CVE-2025-47855
Fortinet Document Library | Upgrade Path Tool