Fortinet FortiClient EMS Authentication Bypass Vulnerability Actively Exploited

TL;DR

A new Fortinet FortiClient EMS vulnerability (CVE-2026-35616, CVSS 9.1) is being actively exploited. The flaw allows unauthenticated attackers to execute code on affected servers.

Overview

There is a new vulnerability in Fortinet FortiClient Enterprise Management Server (EMS) (CVE-2026-35616, CVSS 9.1) that is already being exploited in the wild. This is an improper access control issue that allows an unauthenticated threat actor to bypass authentication and run code or commands through specially crafted API requests.

Affected Products

- FortiClient EMS 7.4.5
- FortiClient EMS 7.4.6
- FortiClient EMS 7.2 – Not affected

Security researchers observed this flaw being used as a zero-day before Fortinet released a patch. More than 2,000 exposed EMS instances have already been identified online, with a large number located in the United States. Because EMS sits at the center of endpoint management, a successful compromise can give an attacker control over managed endpoints and the ability to move deeper into the environment.

This follows closely behind another actively exploited FortiClient EMS vulnerability (CVE-2026-21643), showing a pattern of attackers targeting exposed EMS infrastructure. Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Apply the emergency hotfix for:
  - FortiClient EMS 7.4.5
  - FortiClient EMS 7.4.6
- Upgrade to FortiClient EMS 7.4.7 when available.
- Restrict external access to EMS servers if possible.
- Place EMS behind a VPN or limit access via IP allowlisting.
- Monitor logs for unusual API requests or authentication bypass attempts.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit the EMS API to gain unauthenticated access (CVE-2026-35616).

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

The FortiClient EMS vulnerability threatens any organization using Fortinet endpoint management infrastructure.

- 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