AL2026_13 Fortinet FortiClient EMS Vulnerability Actively Exploited in Attacks (April 10th, 2026)

Description

A critical vulnerability affecting Fortinet **FortiClient Endpoint Management Server (EMS)** is being actively exploited in cyberattacks. The vulnerability, tracked as **CVE-2026-35616**, allows attackers to bypass authentication controls and execute malicious commands on affected systems.

FortiClient EMS is a centralized management platform used by organizations to deploy and manage the FortiClient security agent across enterprise endpoints. If compromised, attackers could gain administrative control over endpoint security policies and potentially pivot deeper into corporate networks.

Security researchers observed exploitation attempts beginning in late March 2026, prompting Fortinet to release emergency patches and urge organizations to update immediately.

Attack Details

The vulnerability stems from improper access control within the FortiClient EMS API layer, enabling attackers to bypass authentication mechanisms.

Key characteristics include:

- **Vulnerability:** CVE-2026-35616 (CVSS score: 9.1), a critical improper access control vulnerability affecting FortiClient EMS.
- **Authentication bypass:** Attackers can send specially crafted HTTP requests to the EMS API to circumvent authentication and authorization checks.
- **Remote code execution:** Successful exploitation may allow attackers to execute unauthorized commands or code on the EMS server.
- **Affected versions:** The flaw impacts FortiClient EMS versions **7.4.5 and 7.4.6**, with fixes provided through hotfixes and an upcoming release.
- **Active exploitation:** Security researchers reported exploitation attempts beginning around **March 31, 2026**, indicating that threat actors quickly weaponized the vulnerability.
- **Related vulnerabilities:** This flaw emerged shortly after another critical FortiClient EMS vulnerability (CVE-2026-21643) was also found to be under active attack.

Because FortiClient EMS manages endpoint security configurations across organizations, compromise could allow attackers to deploy malware, disable endpoint protection, or gain access to managed devices.

Remediation

Organizations using Fortinet endpoint security infrastructure should take the following actions immediately:

- **Apply security updates:** Install the latest Fortinet patches or hotfixes addressing CVE-2026-35616 as soon as possible. Link to the hotfixes can be found below:
  - https://docs.fortinet.com/document/forticlient/7.4.5/ems-release-notes/832484 - for FortiClientEMS 7.4.5
  - https://docs.fortinet.com/document/forticlient/7.4.6/ems-release-notes/832484 - for FortiClientEMS 7.4.6
- **Upgrade affected systems:** Ensure FortiClient EMS instances running versions **7.4.5 or 7.4.6** are updated to patched releases.
- **Restrict administrative access:** Limit access to the EMS management interface to trusted internal networks and authorized administrators only.
- **Monitor server activity:** Review logs for suspicious API requests, unauthorized authentication attempts, or unexpected administrative actions.
- **Network segmentation:** Isolate endpoint management servers from general enterprise networks to reduce the impact of compromise.
- **Threat hunting:** Conduct forensic analysis for indicators of compromise (IOCs) if vulnerable systems were exposed to the internet.
- **Security monitoring:** Implement intrusion detection and continuous monitoring to detect abnormal activity originating from management servers.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2026). *New Fortinet FortiClient EMS flaw (CVE-2026-35616) exploited in attacks.* Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/new-fortinet-forticlient-ems-flaw-cve-2026-35616-exploited-in-attacks/