CYBER ADVISORY

Monday, April 06, 2026 **CAL-CSIC-202604-A-001**

Critical Improper Access Control Zero-Day Vulnerability in FortinetClient EMS under active exploitation

Zero-Day | API Authentication Bypass | Exploited in the Wild | Hotfix Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified CVE-2026-35616 as a critical zero-day vulnerability affecting Fortinet's FortiClientEMS. CVE-2026-35616 has a Common Vulnerability Scoring System (CVSS) v3.1 base score of 9.8.[1] Successful exploitation may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests that bypass API authentication. This can lead to complete compromise of the management server, unauthorized access to sensitive data, and the potential to control managed endpoints. CVE-2026-35616 is actively being exploited as a zero-day vulnerability. Fortinet has since released an advisory confirming the vulnerability being exploited in the wild and has released a hotfix for affected versions.[2]

The Cal-CSIC recommends to apply Fortinet's hotfixes as soon as possible.

For detailed Fortinet's hotfix instructions, refer to the official PSIRT Fortilabs' Security Advisory.[3]

https://fortiguard.fortinet.com/psirt/FG-IR-26-099

Product	Affected Versions
Fortinet FortiClientEMS	FortinetClientEMS 7.4 v.7.5.6 through 7.4.6

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References:

[1] NVD; "CVE-2026-35616 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-35616; accessed 06 April 2026
[2] Tenable; "Zero-Day Vulnerability Exploited (CVE-2026-35616") https://www.tenable.com/blog/cve-2026-35616-fortinet-forticlientems-improper-access-control-vulnerability-exploited-in-the; accessed 06 April 2026
[3] PSIRT; "API authentication and authorization bypass"; https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865; accessed 06 April 2026