



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Actively Exploited Critical Vulnerability in Fortinet FortiClient EMS

Tracking #:432318720

Date:04-04-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Fortinet FortiClient EMS that is actively being exploited in the wild. The flaw allows unauthenticated attackers to bypass API authentication and authorization controls, potentially leading to remote code execution and full system compromise.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-35616
- **Severity:** **Critical** **CVSS Score:** 9.1
- **CWE:** CWE-284 – Improper Access Control
- The vulnerability is caused by improper enforcement of access controls within the FortiClient EMS API. Specifically, the system fails to correctly validate authentication and authorization for certain API requests.
- An attacker can exploit this flaw by sending specially crafted requests to the EMS server, bypassing authentication mechanisms. Successful exploitation enables unauthorized execution of code or commands on the affected system.
- Fortinet has confirmed that this vulnerability is actively being exploited, making it a high-priority risk for affected organizations.

Affected Products

- **FortiClient EMS 7.4**
 - Versions **7.4.5 through 7.4.6** are affected
- **FortiClient EMS 7.2**
 - Not affected

Fixed Versions / Mitigations

- Install the hotfix for FortiClient EMS 7.4.5 and 7.4.6, by following the instructions at:
 - <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 to FortiClient EMS 7.4.7 or later (when available), which includes a permanent fix.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Fortinet.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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