An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2604070224

NCSC Advisory

Fortinet: Critical Improper Access Control Vulnerability in FortiClientEMS

CVE-2026-35616

7th, April 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-35616

Published: 2026-04-04

Vendor: Fortinet

Product: FortiClientEMS

CVSS Score[1]: 9.1

Products Affected

Product	Version
FortiClientEMS	7.4.5 <= 7.4.6

Impact

An improper access control vulnerability in Fortinet FortiClientEMS 7.4.5 through 7.4.6 may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.

Common Weakness Enumeration (CWE)[2]: CWE-284: Improper Access Control

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Fortinet.

As this is a serious vulnerability under active exploitation Fortinet has released an out of band hotfix for both versions of the software that are affected. Instructions on how to access these and install them are available at the following links.

https://docs.fortinet.com/document/forticlient/7.4.6/ems-release-notes/832484

https://docs.fortinet.com/document/forticlient/7.4.5/ems-release-notes/832484

- https://nvd.nist.gov/vuln/detail/CVE-2026-35616
- https://www.cve.org/CVERecord?id=CVE-2026-35616
- https://fortiguard.fortinet.com/psirt/FG-IR-26-099
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-35616