GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

8 April 2026

Advisory 129: Fortinet FortiClient EMS Improper Access Control Vulnerability

Release Date: 6th April 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-35616 is a critical remote code execution (RCE) vulnerability (CVSS 9.8) affecting Fortinet FortiClient Endpoint Management Server (EMS). The flaw is caused by improper access control (CWE-284) in the application's API.

Due to insufficient authentication enforcement, the system fails to properly restrict access to sensitive API endpoints. This allows attackers to send crafted requests that bypass authentication and execute unauthorized commands.

What are the systems affected?

The following version affected;

- Fortinet FortiClient EMS

- Specifically, versions:

- **7.4.5**
- **7.4.6**

What does this mean?

Typical exploitation flow:

1. **Target discovery**
   - Attackers scan for exposed FortiClient EMS servers.
2. **Crafted API request**
   - A specially crafted HTTP request is sent to vulnerable API endpoints.
3. **Authentication bypass**
   - Improper access control allows the request to bypass authentication mechanisms.
4. **Execution of malicious commands**
   - The attacker executes arbitrary commands or code on the EMS server.
5. **Post-exploitation**
   - Attackers may:
     - Gain administrative control
     - Deploy malware or ransomware
     - Move laterally across managed endpoints

This vulnerability requires:

- No authentication
- No user interaction
- Low attack complexity

Mitigation process

CERTVU recommends the following:

1. **Apply Security Updates Immediately**
   - Install Fortinet security updates / hotfixes addressing the vulnerability.
   - Follow Fortinet advisory FG-IR-26-099.
2. **Restrict Network Exposure**
   - Do not expose EMS management interfaces to the internet.
3. **Monitor for Indicators of Compromise (IoCs)**

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-35616
3. https://fortiguard.fortinet.com/psirt/FG-IR-26-099

.