

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Fortinet EMS Left Defenseless by CVE-2026-35616

Date of Publication

April 07, 2026

Admiralty Code

A1

TA Number

TA2026090







# Summary

**First Seen:** March 31, 2026

**Affected Products:** Fortinet FortiClient EMS 7.4.5 through 7.4.6

**Impact:** Successful exploitation of CVE-2026-35616 poses a severe risk to organizations that rely on Fortinet FortiClient EMS for centralized endpoint management. Because the vulnerability is pre-authentication, an unauthenticated attacker with network access to the FortiClient EMS server can bypass API authentication and authorization controls without valid credentials. This could result in full privilege escalation, enabling the attacker to execute arbitrary code or system commands on the affected server. Given that FortiClient EMS serves as a centralized management platform for deploying policies, patches, and security configurations to endpoint agents across an enterprise, compromise of this system could provide an attacker with broad lateral access to managed endpoints, facilitate deployment of malicious configurations, or enable persistent access to the target environment.

## CVEs

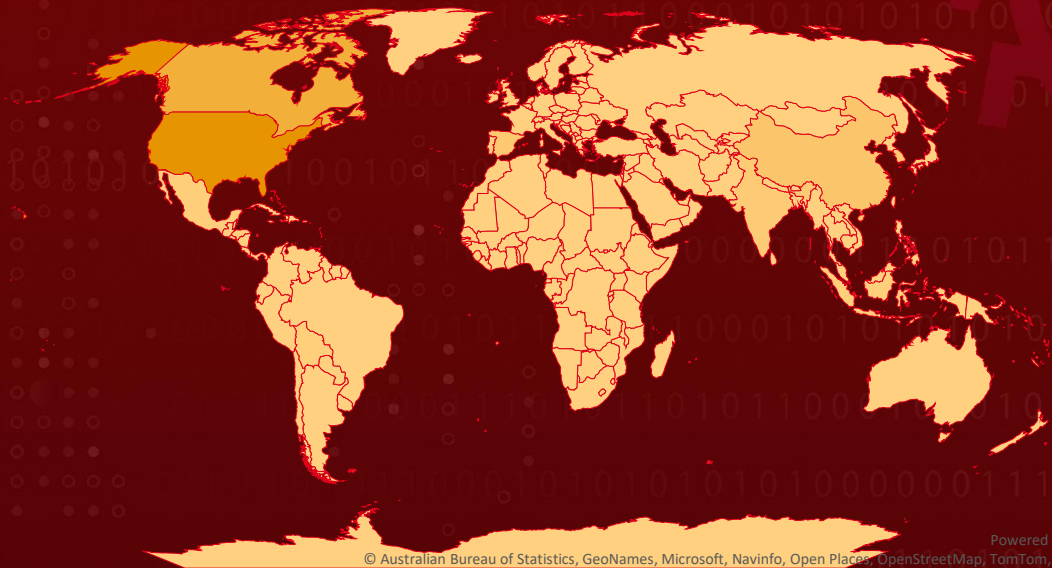
CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-35616	Fortinet FortiClient EMS Improper Access Control Vulnerability	Fortinet FortiClient EMS			
CVE-2026-21643	Fortinet FortiClient EMS Sql Injection Vulnerability	Fortinet FortiClient EMS			

# 🗡️ Attack Regions

Most



Least



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

■ Targeted

■ Non-Targeted

## Vulnerability Details

### #1

Fortinet has issued emergency patches for a critical flaw in FortiClient EMS after confirming it is being actively exploited. The vulnerability, tracked as CVE-2026-35616, affects the system's API, which manages communication between the EMS server and endpoint devices. Due to weak access controls, attackers can send crafted requests that bypass authentication entirely.

### #2

The issue stems from the API failing to properly verify who is making a request and what permissions they have. Because no login or credentials are required, attackers can directly interact with the system, escalate privileges, and run unauthorized commands on the server. This significantly lowers the effort needed to carry out an attack.

### #3

The flaw impacts FortiClient EMS versions 7.4.5 and 7.4.6, while earlier versions, such as the 7.2 branch, remain unaffected. Exploitation was first detected on March 31, 2026, with Fortinet confirming the activity and releasing fixes on April 4. The timing, aligned with the Easter weekend, indicates attackers likely chose a period when security teams were less active to increase their chances of success. This second vulnerability is notably the critical unauthenticated flaw in FortiClient EMS within a matter of weeks, following CVE-2026-21643, which involved SQL injection via the Site header and was also actively exploited.

# Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-35616	Fortinet FortiClient EMS version 7.4.5 through 7.4.6	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*	CWE-284
CVE-2026-21643	Fortinet FortiClient EMS 7.4.4	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*	CWE-89

## Recommendations



**Immediate Patching:** Apply the official fixes for affected FortiClient EMS versions (7.4.5–7.4.6) without delay. Systems left unpatched remain directly exposed to unauthenticated exploitation.



**Restrict API Exposure:** Limit access to the EMS API by enforcing network-level controls. Allow only trusted IP ranges and internal systems to communicate with the EMS server. Avoid exposing the API to the public internet.



**Implement Strong Access Controls:** Enforce strict authentication and authorization checks across all API endpoints. Validate every request, even those assumed to be internal, and remove implicit trust within the network.



**Restrict Network Access to FortiClient EMS:** As an immediate mitigation measure, organizations should ensure that the FortiClient EMS management interface and API endpoints are not directly exposed to the internet. Access should be restricted to trusted internal networks or VPN-connected segments using firewall rules and access control lists. This reduces the attack surface available to unauthenticated remote attackers.



**Audit Logs and Investigate for Signs of Compromise:** Given the confirmed zero-day exploitation window beginning March 31, 2026, security teams should review FortiClient EMS server logs, web server access logs, and network traffic records for anomalous API requests, unauthorized configuration changes, or unexpected command execution. Any indicators of compromise should trigger a full incident response investigation, including examination of managed endpoints for signs of lateral movement or persistence mechanisms.



## Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Privilege Escalation	<u>T1068</u> : Exploitation for Privilege Escalation	
Execution	<u>T1059</u> : Command and Scripting Interpreter	
Persistence	<u>T1505</u> : Server Software Component	
Lateral Movement	<u>T1072</u> : Software Deployment Tools	



### Patch Links

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

<https://fortiguard.fortinet.com/psirt/FG-IR-25-1142>



### References

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

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

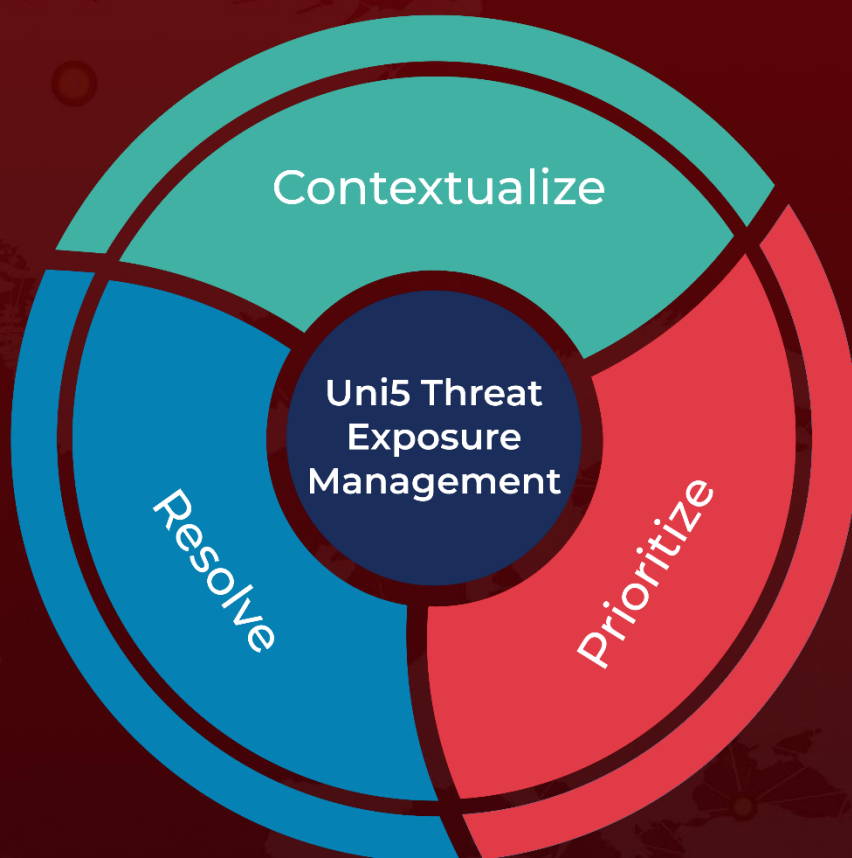
<https://fortiguard.fortinet.com/psirt/FG-IR-25-1142>



# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**April 07, 2026 • 6:00 AM**

© 2026 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)