

Threat Level

**R** Red

Hiveforce Labs

## THREAT ADVISORY

**並 VULNERABILITY REPORT** 

CVE-2025-25256: Fortinet Rushes to Patch High-Risk FortiSIEM Vulnerability

**Date of Publication** 

August 14, 2025

**Admiralty Code** 

**A1** 

**TA Number** 

TA2025249

# **Summary**

**Discovered On:** August 12, 2025 **Affected Product:** Fortinet FortiSIEM

**Impact:** A critical flaw in Fortinet's FortiSIEM platform, tracked as CVE-2025-25256 is allowing remote attackers to run unauthorized commands without needing to log in. The issue stems from a command injection vulnerability in how the system processes certain CLI requests, putting security operations data and infrastructure at serious risk. With proof-of-concept exploit code already available, organizations are urged to patch immediately, restrict access to management interfaces, and closely monitor for suspicious activity to prevent compromise.

#### **⇔CVE**

0	CVE	NAME	AFFECTED PRODUCT	ZERO- DAY	CISA KEV	PATCH
0	CVE-2025- 25256	Fortinet FortiSIEM OS Command Injection Vulnerability	Fortinet FortiSIEM	8	8	<b>⊘</b>

# **Vulnerability Details**

#1

Fortinet has addressed a critical vulnerability in its FortiSIEM platform, warning that exploit code is already circulating in the wild. Tracked as CVE-2025-25256, the flaw allows remote, unauthenticated attackers to execute arbitrary commands on targeted systems through specially crafted CLI requests, making it a high-risk threat for any unpatched deployment.

FortiSIEM serves as Fortinet's Security Information and Event Management (SIEM) solution, providing security teams with advanced threat detection, incident response, and compliance monitoring capabilities. A breach of such a platform could have far-reaching consequences, as it sits at the heart of an organization's security operations.

The vulnerability stems from improper neutralization of special elements in OS commands, effectively creating a command injection pathway. If exploited, it could grant an attacker the ability to run unauthorized code or commands, potentially compromising the integrity and security of the affected environment.

This warning comes just a day after GreyNoise reported a surge in brute-force attacks against Fortinet SSL VPN appliances earlier this month, followed by a shift in targeting toward FortiManager. With a proof-of-concept exploit for CVE-2025-25256 already available, Fortinet is urging all customers to upgrade their FortiSIEM installations to the latest patched versions without delay.

### Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025- 25256	FortiSIEM Versions 7.3.0 through 7.3.1 7.2.0 through 7.2.5 7.1.0 through 7.1.7 7.0.0 through 7.0.3 6.7.0 through 6.7.9 FortiSIEM 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, and 5.4 All Versions	cpe:2.3:a:fortinet:fortisiem:*: *:*:*:*:*:*	CWE-78

### Recommendations



**Update immediately:** If you use FortiSIEM, install the latest security patch for CVE-2025-25256 without delay. This vulnerability already has the exploit code available, so every hour you wait increases the risk.



**Workaround:** Until you can apply the official patch, restrict access to the phMonitor port (7900) so only trusted systems or networks can reach it. This can be done by adjusting firewall rules or access control lists to block all unnecessary inbound connections.



**Limit exposure:** Where possible, restrict external access to FortiSIEM's management interface to trusted networks or via a VPN.



**Monitor for signs of compromise:** Review recent FortiSIEM logs for any unusual or unauthorized CLI activity. Sudden or unexplained changes may indicate an attempted or successful attack.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

### **Potential MITRE ATT&CK TTPs**

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	<u>T1588.005</u> Exploits	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation

#### **SPATCH Details**

Install the latest version of FortiSIEM to address the flaw.

FortiSIEM 7.3.2 or above

FortiSIEM 7.2.6 or above

FortiSIEM 7.1.8 or above

FortiSIEM 7.0.4 or above

FortiSIEM 6.7.10 or above

Link:

https://fortiguard.fortinet.com/psirt/FG-IR-25-152

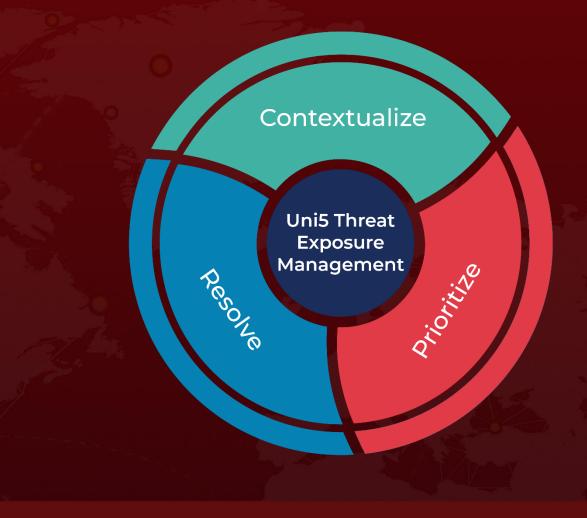
#### **References**

https://fortiguard.fortinet.com/psirt/FG-IR-25-152

### What Next?

At <u>Hive Pro</u>, 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 <u>HivePro Uni5</u>: Threat Exposure Management Platform.



REPORT GENERATED ON

August 14, 2025 5:10 AM

