Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Unauthenticated SQL Injection Flaw in Fortinet FortiWeb

Date of Publication	Admiralty Code	TA Number
July 14, 2025	A1	TA2025217

Summary

First Seen: July 8, 2025
Affected Product: Fortinet FortiWeb
Impact: CVE-2025-25257 is a critical unauthenticated SQL injection vulnerability affecting Fortinet FortiWeb appliances. Exploiting improperly sanitized user inputs in the administrative API, attackers can execute arbitrary SQL commands via the HTTP/HTTPS interface without authentication. The SQL injection can be escalated to Remote Code Execution (RCE) by writing malicious files to the underlying system. Public proof-of-concept (PoC) exploit code is available, and immediate patching is strongly recommended to prevent exploitation.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-25257	Fortinet FortiWeb Unauthenticated SQL Injection Vulnerability	Fortinet FortiWeb	✗	✗	✓

Vulnerability Details

#1

CVE-2025-25257 is a critical security vulnerability discovered in Fortinet's FortiWeb web application firewall, a product widely used to protect web applications from various threats. The flaw is an SQL injection vulnerability found in the Fabric Connector component of FortiWeb's administrative interface. Due to improper input sanitization, an attacker can inject malicious SQL commands by manipulating certain HTTP headers, specifically the Authorization, Bearer header, in unauthenticated requests. This allows attackers to interact directly with the underlying database, bypassing authentication controls entirely.

#2

This vulnerability is particularly dangerous because it requires no authentication and can be exploited remotely, making any exposed management interface a high-value target. Successful exploitation allows attackers to execute arbitrary SQL commands, which can result in unauthorized access to, modification, or deletion of database records. In some cases, attackers may be able to escalate the attack to achieve remote code execution under the context of the application, potentially leading to full system compromise.

#3

As of mid-July 2025, proof-of-concept exploit code is publicly available, and security researchers have demonstrated that remote code execution is possible. While there are no confirmed reports of active exploitation in the wild, the critical nature of the flaw and the history of Fortinet products being targeted by attackers underscore the urgency of applying the available patches and reviewing the security of any exposed management interfaces.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-25257	Fortinet FortiWeb versions: 7.6.0 - 7.6.3 7.4.0 - 7.4.7 7.2.0 - 7.2.10 7.0.0 - 7.0.10	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	CWE-89

Recommendations

Apply Patches Immediately: Fortinet has released patches addressing this vulnerability. Upgrade to FortiWeb versions 7.6.4, 7.4.8, 7.2.11, or 7.0.11 (or later) as soon as possible to eliminate the risk of exploitation.

Restrict Administrative Interface Access: Limit access to the FortiWeb administrative HTTP/HTTPS interfaces by using IP allowlisting or VPN access. Disable administrative access from untrusted networks wherever feasible.

Monitor Traffic: Inspect logs for abnormal activity targeting the /api/fabric/* endpoints and monitor for unexpected file creation, especially .pth files and changes to the ml-draw.py script.

Implement Web Application Firewall (WAF) Protections: Enable or update WAF rules to block suspicious requests and SQL injection attempts targeting FortiWeb endpoints.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	TA0001 Initial Access	TA0004 Privilege Escalation
TA0005 Defense Evasion	T1059.006 Python	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation
T1070 Indicator Removal	T1588 Obtain Capabilities	T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities

Patch Details

Upgrade to FortiWeb versions 7.6.4, 7.4.8, 7.2.11, or 7.0.11 or later.

Link:
https://fortiguard.fortinet.com/psirt/FG-IR-25-151

References

https://labs.watchtowr.com/pre-auth-sql-injection-to-rce-fortinet-fortiweb-fabric-connector-cve-2025-25257/

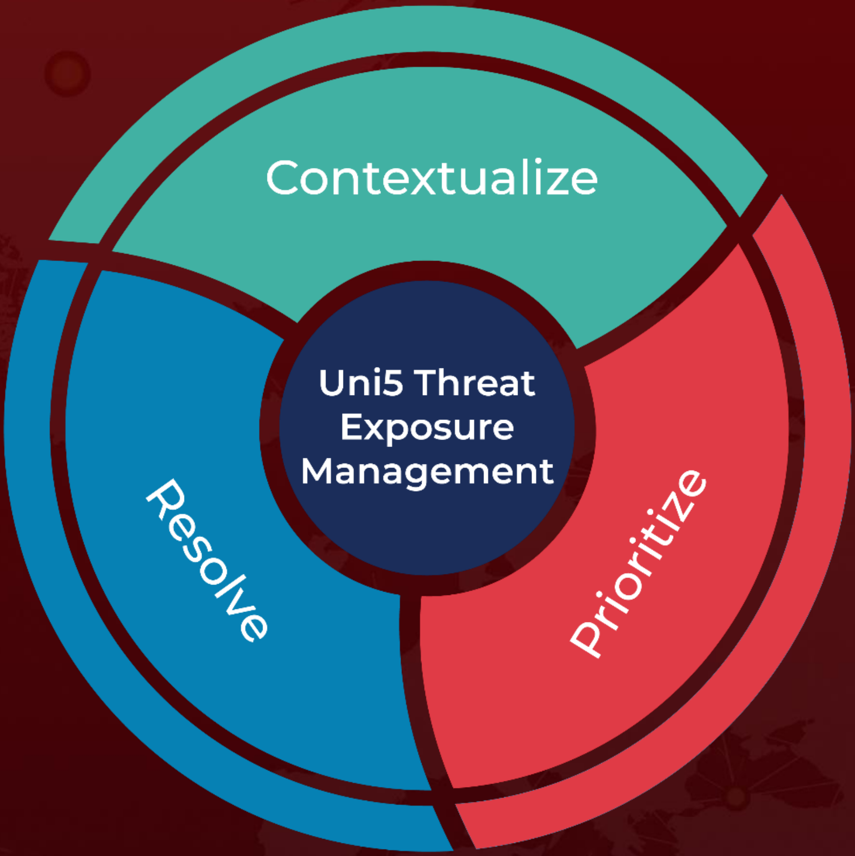
https://pwner.gg/blog/2025-07-10-fortiweb-fabric-rce

https://hivepro.com/threat-advisory/exploited-in-the-wild-fortinet-urges-patch-for-critical-zero-day/

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

July 14, 2025 • 6:30 AM

More at www.hivepro.com