Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

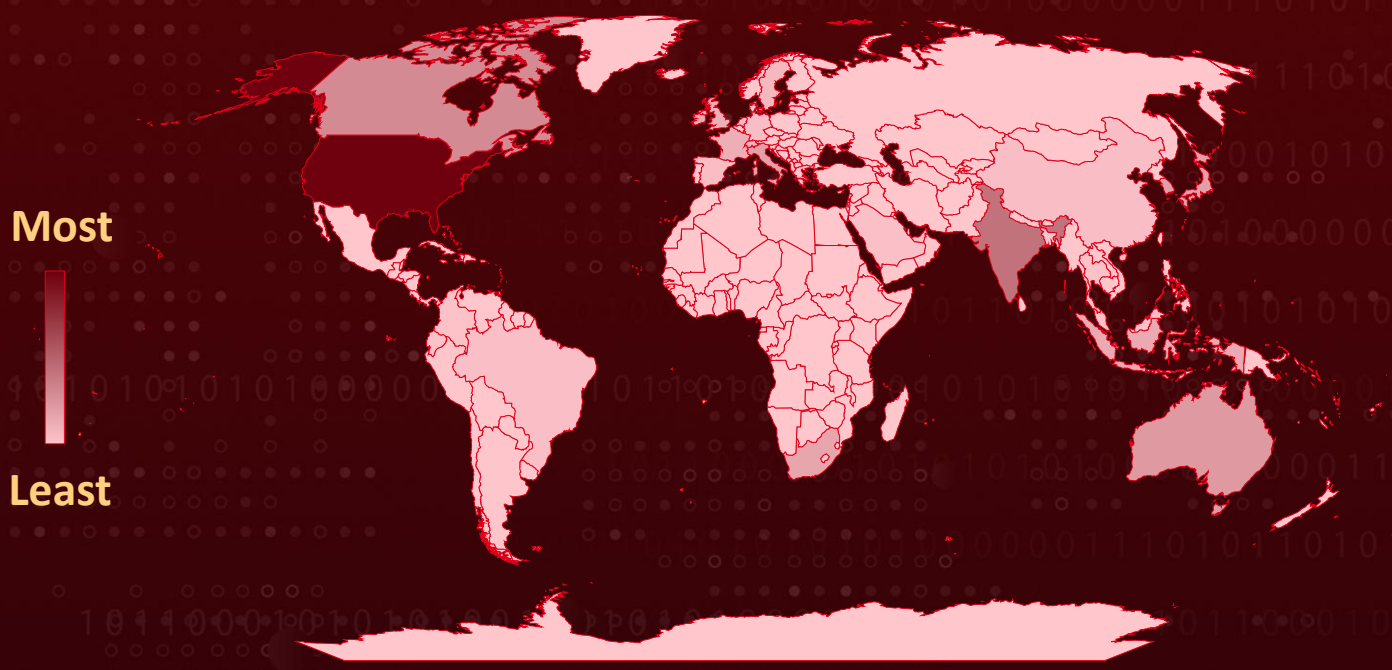
FortiWeb Hijack: The Hidden Vulnerability Fueling Admin Account Creation

Date of Publication	Admiralty Code	TA Number
November 17, 2025	A1	TA2025349

Summary

First Seen: October 2025
Affected Products: Fortinet FortiWeb
Impact: A critical flaw in FortiWeb, tracked as CVE-2025-64446, has allowed attackers to silently infiltrate devices, impersonate administrators, and establish their own persistent access, prompting Fortinet to rush out a fix. By exploiting a path traversal bug and a broken authentication mechanism, threat actors could seize full control with a single crafted request. With exploitation already happening at scale, users are urged to update immediately, secure exposed interfaces, and review their systems for suspicious admin accounts or unexpected changes to ensure they haven't been compromised.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-64446	Fortinet FortiWeb Path Traversal Vulnerability	Fortinet FortiWeb	✓	✓	✓

Vulnerability Details

#1 Fortinet has patched a critical flaw in FortiWeb, its web application firewall, after discovering that attackers were actively exploiting it at scale. Tracked as CVE-2025-64446, this vulnerability is a severe path traversal bug that allows unauthenticated attackers to create new administrative users on exposed devices. The flaw has been under active exploitation since early October, with attackers disguising malicious HTTP POST requests as legitimate traffic to slip past defenses.

#2 The attack begins with a crafted POST request to the endpoint, which is used to trigger the path traversal. By starting the URI with a valid FortiWeb API path, the attacker gains access to the underlying fwbcgi executable. This sets the stage for the second phase, where the attacker exploits a weakness in the fwbcgi binary's authentication handling. The cgi_auth() function, which should enforce authentication, simply accepts user identity details supplied by the attacker through a base64-encoded CGIINFO header, without validating them.

#3 From this header, the function extracts four key values: username, profname, vdom, and loginname. Because FortiWeb devices share the same attributes for their built-in admin account, attackers can reliably impersonate it by supplying the right JSON structure. Once the system processes this fake identity, every action performed afterward is treated as if it came from a legitimate administrator. This gives the attacker full control, including the ability to create persistent admin accounts and make unauthorized changes that can survive reboots.

#4 Fortinet urges customers to disable HTTP and HTTPS on internet-facing interfaces as a temporary workaround. Users should also review their device configurations and audit logs for unexpected changes or unknown administrator accounts. To fully eliminate the risk, upgrading to the latest fixed version is strongly recommended.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-64446	Fortinet FortiWeb 8.0 - 8.0.0 through 8.0.1 Fortinet FortiWeb 7.6 - 7.6.0 through 7.6.4 Fortinet FortiWeb 7.4 - 7.4.0 through 7.4.9 Fortinet FortiWeb 7.2 - 7.2.0 through 7.2.11 Fortinet FortiWeb 7.0 - 7.0.0 through 7.0.11	cpe:2.3:a:fortinet:forti web:*:*:*:*:*:*:*:*	CWE-23

Recommendations

- **Update Immediately:** Install the latest fixed FortiWeb version as soon as possible. This is the only reliable way to fully protect your device from ongoing attacks.
- **Limit Exposure:** Temporarily disable HTTP and HTTPS access on any internet-facing FortiWeb interfaces until the update is applied. This reduces the attacker's entry points.
- **Check for Suspicious Admin Accounts:** Review all administrator profiles on your device. Remove any accounts you don't recognize and investigate when they were created.
- **Strengthen Access Controls:** If possible, restrict management access to trusted IP addresses only, and ensure MFA is enabled for all admin accounts.
- **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	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation	T1098 Account Manipulation	T1106 Native API
T1036 Masquerading	T1027 Obfuscated Files or Information		

Patch Details

Update your Fortinet FortiWeb to the latest version.
FortiWeb 8.0 - Upgrade to 8.0.2 or above
FortiWeb 7.6 - Upgrade to 7.6.5 or above
FortiWeb 7.4 - Upgrade to 7.4.10 or above
FortiWeb 7.2 - Upgrade to 7.2.12 or above
FortiWeb 7.0 - Upgrade to 7.0.12 or above

Link: https://fortiguard.fortinet.com/psirt/FG-IR-25-910

References

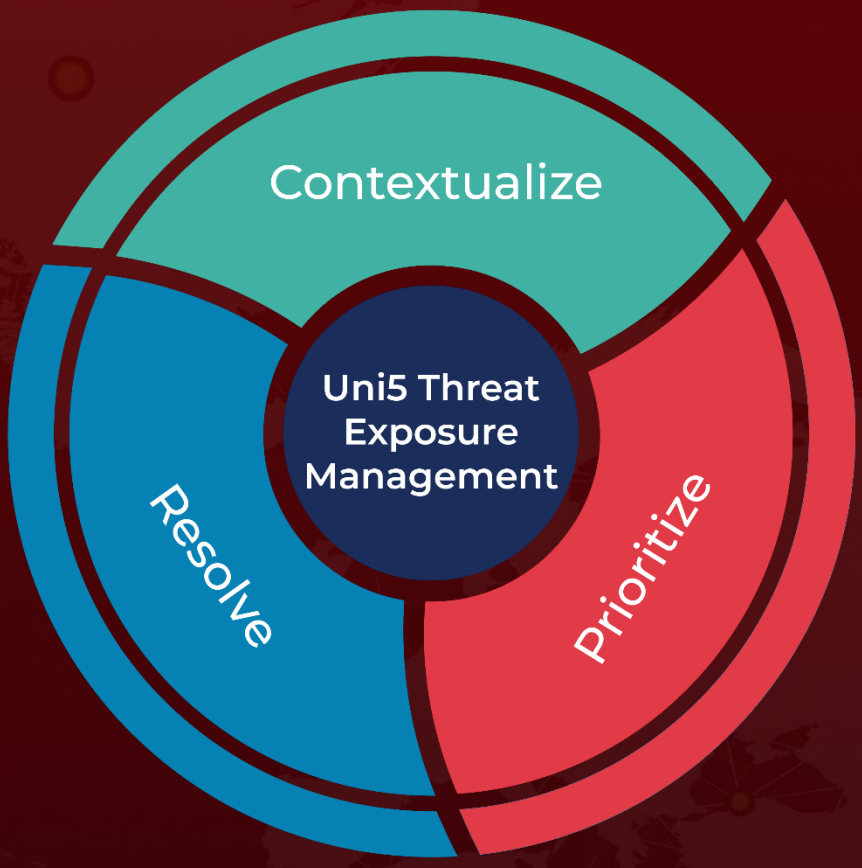
https://fortiguard.fortinet.com/psirt/FG-IR-25-910

https://labs.watchtowr.com/when-the-impersonation-function-gets-used-to-impersonate-users-fortinet-fortiweb-auth-bypass/

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

November 17, 2025 • 7:00 AM

More at www.hivepro.com