Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

WordPress Sites Under Siege by Old Critical Flaws

Date of Publication	Admiralty Code	TA Number
October 28, 2025	A1	TA2025328

Summary

First Seen: September 25th, 2024
Affected Products: GutenKit and Hunk Companion WordPress plugins
Impact: Attackers are aggressively exploiting three critical flaws, CVE-2024-9234, CVE-2024-9707, and CVE-2024-11972, in the GutenKit and Hunk Companion WordPress plugins, providing a direct path to install malicious plugins, execute remote code, and silently take control of websites. The campaign surged in October 2025, showing that even year-old vulnerabilities can become a major threat when updates are ignored. With weaponized plugins hosted on platforms like GitHub, attackers can steal data, maintain persistence, and even create fake admin accounts. Keeping plugins updated and maintaining strong security controls is key to staying ahead of ongoing exploitation attempts.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-9234	WordPress GutenKit Plugin Unauthenticated Arbitrary File Upload Vulnerability	WordPress GutenKit Plugin	✗	✗	✓
CVE-2024-9707	WordPress Hunk Companion Plugin Unauthenticated Arbitrary Plugin Activation Vulnerability	WordPress Hunk Companion Plugin	✗	✗	✓
CVE-2024-11972	WordPress Hunk Companion Plugin Unauthenticated Arbitrary Plugin Activation Vulnerability	WordPress Hunk Companion Plugin	✗	✗	✓

Vulnerability Details

#1

A widespread exploitation campaign is actively targeting WordPress sites that run the GutenKit and Hunk Companion plugins, taking advantage of long-standing, high-severity bugs to achieve remote code execution. Attackers are using unauthenticated API abuses with weaponized plugins to drop code on vulnerable installs, gain persistence, and move laterally inside compromised environments.

#2

Three critical flaws are central to the campaign: CVE-2024-9234 affects GutenKit's install/activate routine and permits arbitrary file uploads and plugin installation when capability checks are missing. CVE-2024-9707 and CVE-2024-11972 impact Hunk Companion's REST endpoint across older releases, allowing unauthorized plugin installation and activation. The latter is effectively a bypass of the earlier issue, making exploitation easier when either weakness is present.

#3

In observed attacks, threat actors craft a seemingly innocuous template-import POST to the Hunk Companion endpoint but embed plugin objects and an allPlugins array that reference a weaponized plugin. If processed, the endpoint registers or loads those plugin paths, enabling the attacker to write and execute code. It was also found that a GitHub-hosted ZIP called "up" that contains obfuscated scripts for uploading, downloading, deleting files, changing permissions, and an All-in-One-SEO-disguised, password-protected script that automatically grants the attacker admin access. When a full admin backdoor isn't available, attackers often fall back to deploying a vulnerable wp-query-console plugin to achieve unauthenticated RCE.

#4

Site owners should treat this as urgent, update GutenKit, Hunk Companion, and all plugins to the vendor's latest releases, remove or disable unused plugins, and scan for unexpected admin accounts, unfamiliar plugins, or odd file additions. Review access logs for suspicious POSTs to /wp-json/hc/v1/themehunk-import and related endpoints. Note that attackers launched a mass campaign on October 8 - 9, 2025, demonstrating that even long-disclosed vulnerabilities remain actively exploited in the wild; patching now prevents you from becoming the next victim. Public proof-of-concept (PoC) code for these flaws is available, which makes quick patching even more important.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-9234	GutenKit Version Prior to 2.1.1	cpe:2.3:a:wpmet:gutenkit:*:*:*:*:*:*:*:*	CWE-862
CVE-2024-9707	Hunk Companion Version Before and 1.8.4	cpe:2.3:a:themehunk:hunk_companion:*:*:*:*:*:wordpress:*:*	CWE-862
CVE-2024-11972	Hunk Companion Version Before and 1.8.5	cpe:2.3:a:themehunk:hunk_companion:*:*:*:*:*:wordpress:*:*	-

Recommendations

Keep Plugins Updated: Immediately update all plugins and themes to their latest versions. In particular, upgrade GutenKit to version 2.1.1 and Hunk Companion to version 1.9.0 to close the critical security gaps exploited in recent attacks.

Remove Unneeded Plugins: Delete any plugins you are not actively using. Fewer plugins mean fewer opportunities for attackers to sneak in or hide malicious code.

Review Server and Access Logs: Keep an eye on logs for unusual POST requests to endpoints related to plugin installation or imports. Early detection can stop attackers before serious damage occurs.

Protect Admin Access: Restrict admin rights to trusted users only. Use strong, unique passwords along with multi-factor authentication to prevent unauthorized access.

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	TA0005 Defense Evasion
TA0007 Discovery	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter
T1027 Obfuscated Files or Information	T1083 File and Directory Discovery	T1190 Exploit Public-Facing Application	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	13[.]218[.]47[.]110, 3[.]10[.]141[.]23, 52[.]56[.]47[.]51, 18[.]219[.]237[.]98, 18[.]116[.]40[.]45, 119[.]34[.]179[.]21, 194[.]87[.]29[.]184, 3[.]133[.]135[.]47, 3[.]141[.]28[.]47, 3[.]85[.]107[.]39, 3[.]148[.]175[.]195, 193[.]84[.]71[.]244, 3[.]147[.]6[.]140, 3[.]144[.]26[.]200, 193[.]233[.]134[.]136
IPv6	2600[:]1f16[:]234[:]9300[:]70c6[:]9e26[:]de1a[:]7696, 2600[:]1f16[:]234[:]9300[:]f71[:]bed2[:]11e5[:]4080

TYPE	VALUE
Domains	ls.fatec[.]info, dari-slideshow[.]ru, zarjavelli[.]ru, korobushkin[.]ru, drschischka[.]at, dpaxt[.]io, cta.imasync[.]com, catbox[.]moe
Plugin Directories	up / up.zip, background-image-cropper / background-image-cropper.zip, ultra-seo-processor-wp / ultra-seo-processor-wp.zip, oke / oke.zip, wp-query-console

Patch Details

Update your GutenKit and Hunk Companion Plugins to the latest version.
GutenKit Update to Version: 2.1.1
Hunk Companion Update to Version: 1.9.0

Link:
https://wordpress.org/plugins/gutenkit-blocks-addon/
https://wordpress.org/plugins/hunk-companion/

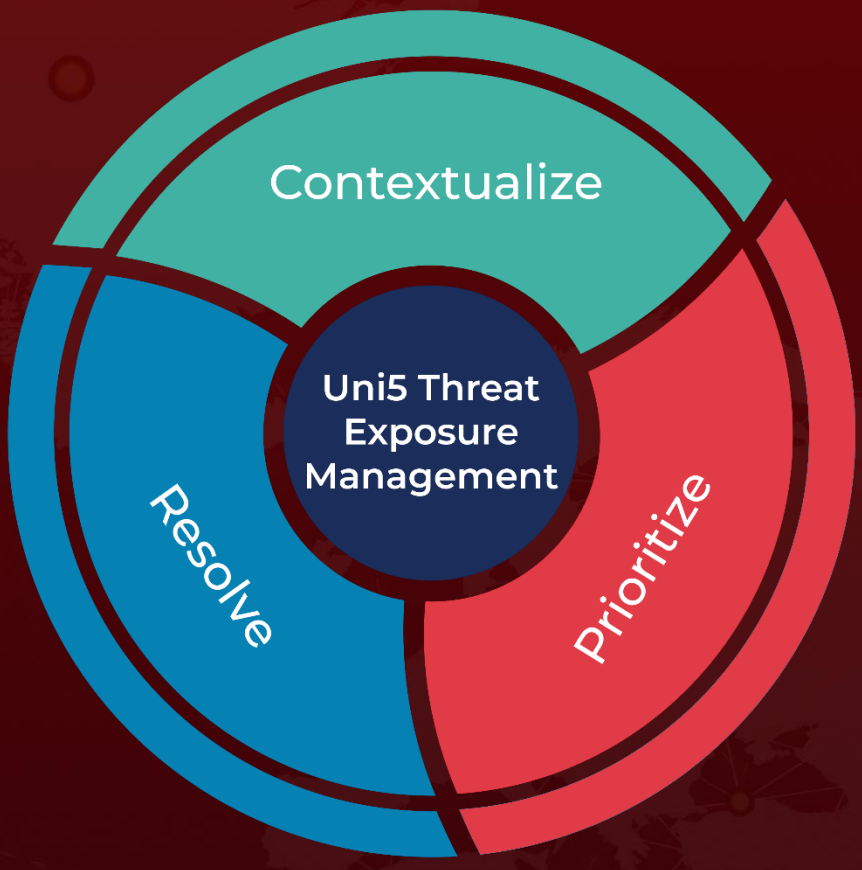
References

https://www.wordfence.com/blog/2025/10/mass-exploit-campaign-targeting-arbitrary-plugin-installation-vulnerabilities/

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

October 28, 2025 • 8:00 AM

More at www.hivepro.com