Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Alone Theme Vulnerability Puts WordPress Sites at Risk

Date of Publication	Admiralty Code	TA Number
July 31, 2025	A1	TA2025236

Summary

First Seen: May 30, 2025
Affected Product: WordPress Alone Theme
Impact: A critical vulnerability (CVE-2025-5394) in the popular Alone - Charity Multipurpose Non-profit WordPress Theme has put thousands of websites at serious risk. Affecting versions up to 7.8.3, this flaw lets attackers upload malicious files without needing to log in, no passwords, no admin rights. By exploiting a weak plugin installer, hackers can install backdoors disguised as innocent-looking plugins, giving them full control over the site. What's more alarming is that exploitation began even before the vulnerability was made public, with over 120,900 attack attempts already blocked. This shows how fast and aggressive threat actors are, and why it's crucial for site owners to patch immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-5394	WordPress Alone Theme Remote Code Execution Vulnerability	WordPress Alone Theme	✗	✗	✓

Vulnerability Details

#1 A critical security vulnerability, CVE-2025-5394 has been discovered in the Alone – Charity Multipurpose Non-profit WordPress Theme, affecting versions up to and including 7.8.3. It allows attackers to upload and execute malicious files on a vulnerable site without authentication. In essence, an attacker can hijack your WordPress site completely without needing a login by exploiting this bug and planting harmful code.

#2 The root of the problem lies in a function within the theme called alone_import_pack_install_plugin(). This function was intended to simplify plugin installations but lacks basic security controls. Critically, it doesn't verify whether the person making the request has administrative privileges, nor does it use WordPress's built-in nonce system to validate requests. This oversight allows unauthenticated users to send a crafted request to install a malicious "plugin" which is a disguised backdoor from a remote server.

#3 Once that backdoor is installed, attackers gain remote code execution (RCE) capabilities, allowing them to run arbitrary commands on your server. From there, they can steal data, deface your website, inject persistent malware, or use your site to launch attacks on others. What makes this particularly dangerous is the ease of exploitation, no user interaction or valid credentials are required. It's essentially an open door to your WordPress admin, left wide open by a flaw in the theme's code.

#4 Even more alarming is that attackers began actively exploiting the vulnerability as early as July 12, 2025, two days before it was publicly disclosed on July 14, 2025. This clearly shows that threat actors are proactively hunting for unpatched sites. The flaw was first identified on May 30, 2025, and the developer released a fix in version 7.8.5 on June 16, 2025. Unfortunately, many websites remained exposed even after the patch became available. Wordfence reported blocking over 120,900 attempted exploits, underlining how widespread and automated these attacks have become. Malicious files used in these campaigns were often disguised with names like wp-classic-editor.zip, hiding backdoors that created secret admin accounts or deployed full file managers, essentially turning affected websites into long-term tools for attackers. With active exploitation underway, patching immediately isn't just recommended, it's absolutely essential.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-5394	WordPress Alone Theme Version 7.8.3 and below	cpe:2.3:a:alone_theme:alone_theme:*:*:*:*:*:*:*:*	CWE-862

Recommendations

Update Immediately: If you're using the Alone theme version 7.8.3 or earlier, update it to the latest patched version right away. This vulnerability is actively being exploited, so every moment your site stays outdated increases the risk of being compromised.

Check Your Site for Suspicious Files: Look for any unfamiliar ZIP files (like wp-classic-editor.zip or background-image-cropper.zip) or PHP files (like accesson.php) in your WordPress directories. These may be signs of a successful attack.

Review User Accounts: Check your WordPress admin panel for unknown users, especially with admin privileges. Attackers often create hidden admin accounts to maintain control over the site.

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	**T1059** Command and Scripting Interpreter	**T1505** Server Software Component	**T1505.003** Web Shell
T1027 Obfuscated Files or Information	**T1204** User Execution	**T1068** Exploitation for Privilege Escalation	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	193[.]84[.]71[.]244, 87[.]120[.]92[.]24, 146[.]19[.]213[.]18,

TYPE	VALUE
IPv4	185[.]159[.]158[.]108, 188[.]215[.]235[.]94, 146[.]70[.]10[.]25, 74[.]118[.]126[.]111, 62[.]133[.]47[.]18, 198[.]145[.]157[.]102
IPv6	2a0b[:]4141[:]820[:]752[::]2
Domains	cta.imasync[.]com, dari-slideshow[.]ru, mc-cilinder[.]nl, wordpress[.]zzna[.]ru, onerange[.]co, Ls[.]fatec[.]info, drschischka[.]at
File Path	/wp-content/plugins, /wp-content/upgrade

Patch Details

Install the latest version 7.8.5 of WordPress Alone Theme to address the flaw.

Link:
https://themeforest.net/item/alone-charity-multipurpose-nonprofit-wordpress-theme/15019939?srsltid=AfmBOooSAqUyZH2ZA9U0DOLSX4pH_drgM0BOTtNABJqo1l-WYwYInBjV

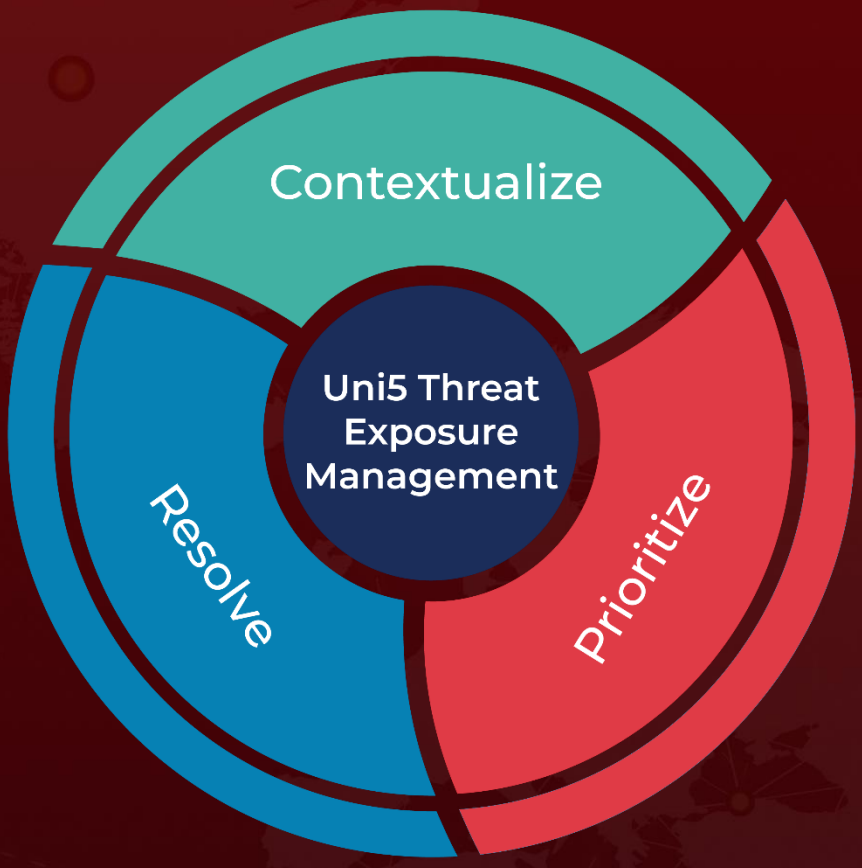
References

https://www.wordfence.com/blog/2025/07/attackers-actively-exploiting-critical-vulnerability-in-alone-theme/

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 31, 2025 • 6:10 AM

More at www.hivepro.com