Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

The Admin Shortcut: King Addons Flaw Under Fire

Date of Publication	Admiralty Code	TA Number
December 4, 2025	A1	TA2025367

Summary

Discovered On: July 24th, 2025
Affected Products: WordPress King Addons for Elementor Plugin
Impact: A critical flaw in the King Addons for Elementor plugin has opened the door for attackers to quietly grant themselves admin access on vulnerable WordPress sites, leading to a surge in real-world exploitation. The bug, tracked as CVE-2025-8489, stems from a simple but dangerous oversight that lets anyone register as an administrator without authentication. Despite a patch arriving in late September, attacks spiked soon after public disclosure, with over 48,400 malicious attempts blocked as attackers rushed to take advantage of unpatched sites. With the threat still active, site owners are urged to update immediately, check for suspicious admin accounts, and tighten their security before attackers turn a harmless registration form into a complete site takeover.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-8489	WordPress King Addons for Elementor Plugin Privilege Escalation Vulnerability	WordPress King Addons for Elementor Plugin	✗	✗	✓

Exploitation Timeline



Vulnerability Details

#1 A severe security flaw in the widely used King Addons for Elementor WordPress plugin has recently drawn attention after being actively exploited in the wild. Tracked as CVE-2025-8489, the bug allows attackers with no authentication whatsoever to escalate their privileges simply by declaring themselves administrators during the registration process. This makes the issue particularly dangerous, as it hands over full site control to anyone who knows how to trigger it.

#2 The vulnerability was first identified on July 24, 2025, and affected more than 10,000 WordPress installations. The core problem lies in how the plugin handles user registration: a missing validation check in the handle_register_ajax() function allows attackers to assign themselves the administrator role without any restrictions. Versions from 24.12.92 through 51.1.14 are impacted. Once inside with admin privileges, an attacker can essentially take over the entire site from altering content and deploying spam to uploading malicious files or redirecting visitors to harmful destinations.

#3 Although a patch was made available on September 25, 2025, exploitation ramped up quickly. More than 48,400 blocked attempts, with attacks beginning on October 31 and intensifying in early November. Public disclosure followed on October 30, giving attackers a window to weaponize the flaw before many sites had updated.

#4 Due to the ongoing exploitation in the wild, site owners are strongly urged to update immediately to the latest secure version, 51.1.35, and verify that no unauthorized administrator accounts exist. Operators of compromised sites should also consider incident response or cleanup assistance to contain further damage. As WordPress environments remain attractive targets, timely patching and active monitoring continue to be essential for maintaining a secure site.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-8489	WordPress King Addons for Elementor Plugin Versions 24.12.92 to 51.1.14	cpe:2.3:a:kingaddons:king_addons_for_elementor_plugin:*:*:*:*:*:*:*:*	CWE-269

Recommendations

Update the Plugin Immediately: Install the latest version of King Addons for Elementor (51.1.35) without delay. This patch fixes the vulnerability, and updating is the fastest way to protect your site.

Review Your User Accounts: Check your WordPress dashboard for any unfamiliar administrator accounts. If you find something suspicious, remove it right away and reset the passwords of trusted accounts.

Back Up Your Site Regularly: Create automatic daily backups so you can quickly restore your site if anything goes wrong. Store backups somewhere safe and not on your live server.

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	**TA0003** Persistence	**TA0004** Privilege Escalation
T1190 Exploit Public-Facing Application	**T1136** Create Account	**T1068** Exploitation for Privilege Escalation	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]61[.]157[.]120, 182[.]8[.]226[.]228, 138[.]199[.]21[.]230, 206[.]238[.]221[.]25
IPv6	2602[:]fa59[:]3[:]424[::]1

Patch Details

Update your King Addons for Elementor Plugin to the latest version 51.1.35.

Link: https://wordpress.org/plugins/king-addons/

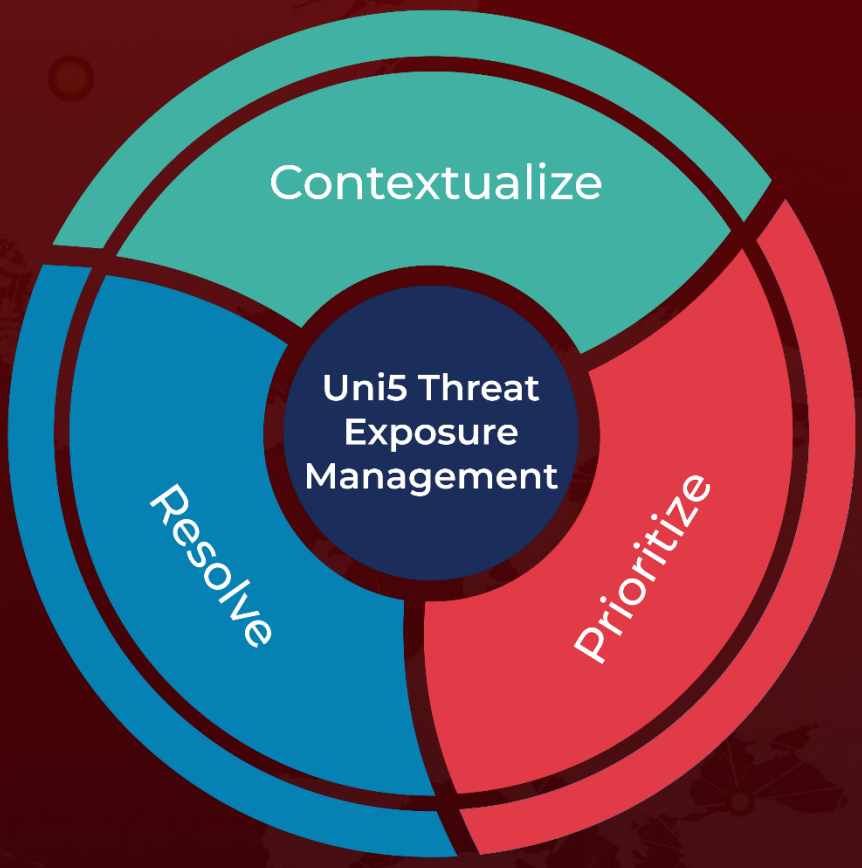
References

https://www.wordfence.com/blog/2025/12/attackers-actively-exploiting-critical-vulnerability-in-king-addons-for-elementor-plugin/

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

December 4, 2025 . 8:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com