Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical WordPress GiveWP Flaw Exposes 100,000+ Sites to RCE & File Deletion

Date of Publication	Admiralty Code	TA Number
August 21, 2024	A2	TA2024320

Summary

First Seen: August 19, 2024
Affected Product: WordPress GiveWP Plugin
Impact: CVE-2024-5932 is a critical vulnerability in the GiveWP plugin for WordPress, allowing unauthenticated attackers to execute arbitrary code and delete files. The vulnerability, with a CVSS score of 10.0, is present in all versions up to 3.14.1 due to improper validation of the give_title parameter. Users are advised to update to version 3.14.2 or later to mitigate the risks of complete site compromise, data loss, and operational disruptions.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-5932	WordPress GiveWP Plugin Remote Code Execution Vulnerability	WordPress GiveWP Plugin	✗	✗	✓

Vulnerability Details

#1

CVE-2024-5932 is a critical remote code execution (RCE) vulnerability that affects the GiveWP plugin for WordPress. This popular donation and fundraising tool is used by over 100,000 active installations. This vulnerability is classified as a PHP Object Injection issue, allowing unauthenticated attackers to execute arbitrary code and delete files on affected WordPress sites.

#2

The vulnerability is caused by the deserialization of untrusted input from the give_title parameter. This allows unauthenticated attackers to inject PHP objects and potentially execute arbitrary code or delete files on the affected WordPress site. This arises because the plugin deserializes user-supplied data without proper sanitization, which can be manipulated to perform malicious actions via PHP magic methods.

#3

If exploited, this vulnerability could allow attackers to take complete control of the affected WordPress site. This could lead to data theft, install malware, website defacement, and other malicious activities. The ability to delete arbitrary files poses significant risks, including potential data loss and operational disruptions. All versions of the GiveWP plugin up to and including 3.14.1 are vulnerable.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-5932	WordPress GiveWP plugin versions prior to 3.14.2	cpe:2.3:a:givewp_plugin:givewp_plugin:*:*:*:*:*:*:*	CWE-502

Recommendations

Update the Plugin: Immediately update the GiveWP plugin to version 3.14.2 or later. Go to your WordPress dashboard, navigate to "Plugins," find GiveWP, and click "Update Now.“

Backup Your Site: Create a full backup of your WordPress site, including the database and files. Use a reliable backup plugin or your hosting provider's backup tools.

Conduct Security Audits: Perform a thorough security audit of your WordPress site to identify any potential vulnerabilities or signs of exploitation.

Implement Web Application Firewalls (WAF): Use a WAF to help filter and monitor HTTP traffic to your WordPress site, providing an additional layer of security against attacks.

Regularly Monitor Logs: Keep an eye on server and application logs for any suspicious activities that could indicate attempts to exploit the vulnerability.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0040 Impact	TA0043 Reconnaissance	TA0004 Privilege Escalation
TA0042 Resource Development	T1588.005 Exploits	T1059 Command and Scripting Interpreter	T1485 Data Destruction
T1068 Exploitation for Privilege Escalation	T1595 Active Scanning	T1588 Obtain Capabilities	T1588.006 Vulnerabilities

Patch Details

Update the WordPress GiveWP plugin to a version 3.14.2 or later versions

Link:
https://wordpress.org/plugins/give/

References

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/give/givewp-donation-plugin-and-fundraising-platform-3141-unauthenticated-php-object-injection-to-remote-code-execution

https://www.wordfence.com/blog/2024/08/4998-bounty-awarded-and-100000-wordpress-sites-protected-against-unauthenticated-remote-code-execution-vulnerability-patched-in-givewp-wordpress-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.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

August 21, 2024 • 3:30 AM

More at www.hivepro.com