Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical XSS Flaw Discovered in WP Statistics Impacting 600K Sites

Date of Publication	Admiralty Code	TA Number
March 15, 2024	A1	TA2024103

Summary

First Seen: March 11, 2024
Affected Platform: WordPress
Impact: A critical Cross-Site Scripting (XSS) vulnerability (CVE-2024-2194) in WP Statistics plugin, allowing attackers to inject malicious code via the URL parameter. With over 600,000 installations, the flaw poses severe risks, enabling unauthorized script execution and potential data theft or site compromise. Update promptly to patched versions to prevent potential exploitation.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-2194	WordPress WP Statistics plugin Cross-Site Scripting Vulnerability	WordPress WP Statistics plugin	✗	✗	✓

Vulnerability Details

#1 A critical vulnerability has been discovered in the widely used WP Statistics plugin, identified as CVE-2024-2194. This flaw, classified as a stored cross-site scripting (XSS) issue, allows attackers to insert malicious code into WordPress websites through the URL search parameter.

#2 The flaw affects all versions of the plugin up to and including 14.5 due to inadequate input sanitization and output escaping. Consequently, unauthenticated attackers can inject arbitrary web scripts onto pages, which execute whenever a user accesses the affected page.

#3

WP Statistics, a popular plugin with over 600,000 installations, provides site owners with insights into visitor traffic and other analytics. The threat is severe due to its wide impact, as many websites could be vulnerable, and attackers don't need login credentials to exploit the flaw. XSS attacks can result in various consequences, including data theft, redirection to harmful sites, creation of unauthorized accounts, and more.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-2194	WordPress WP Statistics Plugin all versions up to 14.5	cpe:2.3:a:wp_statistics_plugin:wp_statistics_plugin:14.0:*:*:*:*:*:*:*	CWE-79

Recommendations

Update Immediately: Ensure that the WP Statistics plugin on your WordPress website is updated to the latest patched version as soon as possible. This update should include fixes for the identified vulnerability (CVE-2024-2194) to prevent attackers from exploiting it.

Regularly Monitor for Updates: Stay vigilant about plugin updates and security patches released by plugin developers. Frequently check for updates for all plugins and themes installed on your WordPress site to promptly address any security vulnerabilities that may arise.

Implement Security Measures: Consider implementing additional security measures, such as installing a reputable security plugins, to provide enhanced protection against hacks, malware, and other security threats. These security plugins often offer features such as firewall protection, malware scanning, and login security enhancements.

Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0001 Initial Access	T1059 Command and Scripting Interpreter
T1588 Obtain Capabilities	T1189 Drive-by Compromise	T1588.005 Exploits	T1588.006 Vulnerabilities

Patch Details

Update WP Statistics to version 14.5.1, or to the latest version

Links:
https://wordpress.org/plugins/wp-statistics/

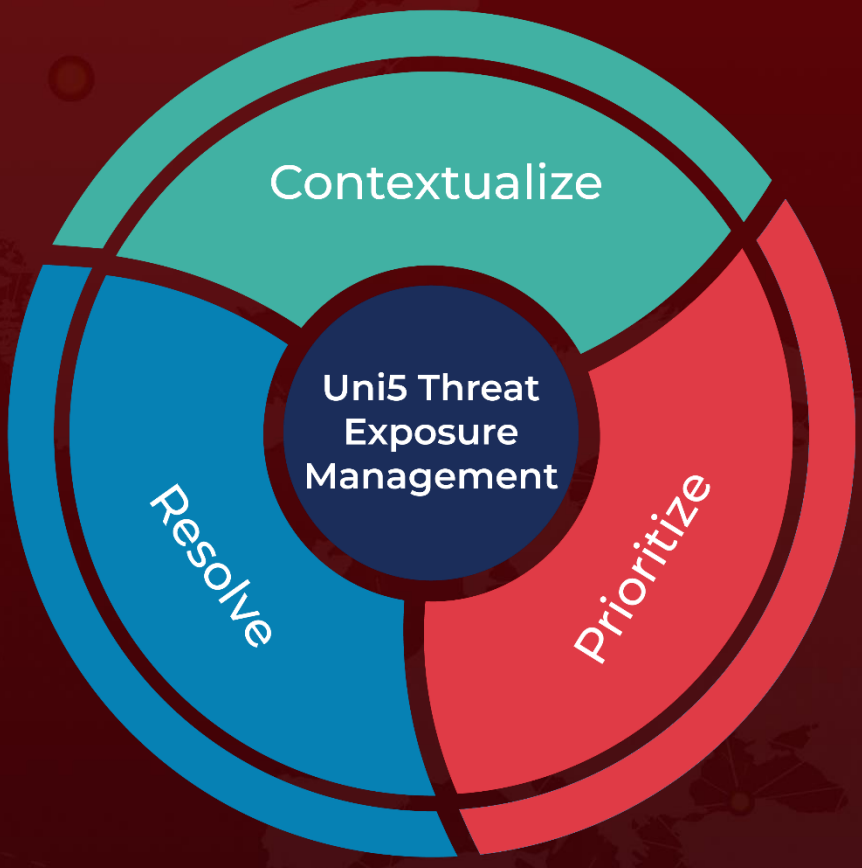
References

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-statistics/wp-statistics-145-unauthenticated-stored-cross-site-scripting

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

March 15, 2024 • 2:30 AM

More at www.hivepro.com