Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Hackers Target WooCommerce Payments Plugin to Hijack Websites

Date of Publication	Admiralty Code	TA Number
July 18 , 2023	A1	TA2023303

Summary

First Seen: March 23, 2023
Affected Product: WordPress WooCommerce Payments plugin
Impact: Cybercriminals are orchestrating a widespread campaign to exploit a pivotal WooCommerce Payments plugin, thereby acquiring the privileges of various users, including those with administrator status, on susceptible WordPress installations.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-28121	WordPress Authentication Bypass Vulnerability	WordPress WooCommerce Payments plugin	☒	☒	✓

Vulnerability Details

#1

The WooCommerce Payments plugin is an immensely popular WordPress plugin that enables websites to accept credit and debit card payments within their WooCommerce stores. This plugin boasts an impressive user base of over 600,000 active installations. However, a critical severity vulnerability known as CVE-2023-28121 with CVSS score of 9.8 has been discovered, posing a threat to all the integrated websites. This vulnerability allows for authentication bypass via the determine_current_user_for_platform_checkout function.

#2

Exploiting this flaw allows remote users to impersonate administrators, granting unauthenticated attackers the power to impersonate various users and carry out actions under the guise of the impersonated user. Such actions have the potential to lead to a complete takeover of the targeted website.

#3

The severity of this vulnerability became apparent as large-scale attacks, attributed to CVE-2023-28121, commenced on Thursday, July 14, 2023, and persisted throughout the weekend. These attacks reached their peak on Saturday, July 16, 2023, with a staggering 1.3 million assault attempts recorded against 157,000 websites. The exploit leverages the aforementioned vulnerability to deploy the WP Console plugin, a tool that, in the hands of an administrator, allows for code execution. However, in the hands of attackers, it serves as a means to execute malicious code and introduce a file uploader, establishing a persistent presence on the compromised systems.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-28121	WordPress WooCommerce Payments plugin version: 4.8.0 - 5.6.1	cpe:2.3:a:automattic:woocommerce_payments:*:*:*:*:*:wordpress:*:*	CWE-287

Recommendations

It is strongly recommended to update the WooCommerce Payments plugin to version 5.6.2 or any newer version that includes **patches** and fixes for identified vulnerabilities. Keeping your plugin up to date ensures that you benefit from the latest security enhancements and safeguards against potential exploits.

Thoroughly examine the data on your site, including integrated plugins, to identify and eliminate any malicious content or hidden backdoors. Conduct a comprehensive review of all administrator accounts, promptly deleting any unfamiliar or unauthorized accounts that may pose a security risk.

Implement a complete password reset for all administrators and users. It is advisable to take advantage of the new password reset feature that will be released by the plugin developers for user passwords.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0040 Impact	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	194.169.175[.]93, 103.102.153[.]17, 79.137.202[.]106, 193.169.194[.]63, 79.137.207[.]224, 193.169.195[.]64
IPv6	2a10:cc45:100::5474:5a49:bfd6:2007

Patch Details

In order to mitigate the vulnerability, it is imperative to upgrade to version 5.6.2 or a subsequent patched release. The necessary plugin version can be effortlessly updated through the WordPress Admin dashboard.

Link:
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/woocommerce-payments/woocommerce-payments-561-authentication-bypass-and-privilege-escalation

References

https://www.wordfence.com/blog/2023/07/massive-targeted-exploit-campaign-against-woocommerce-payments-underway/

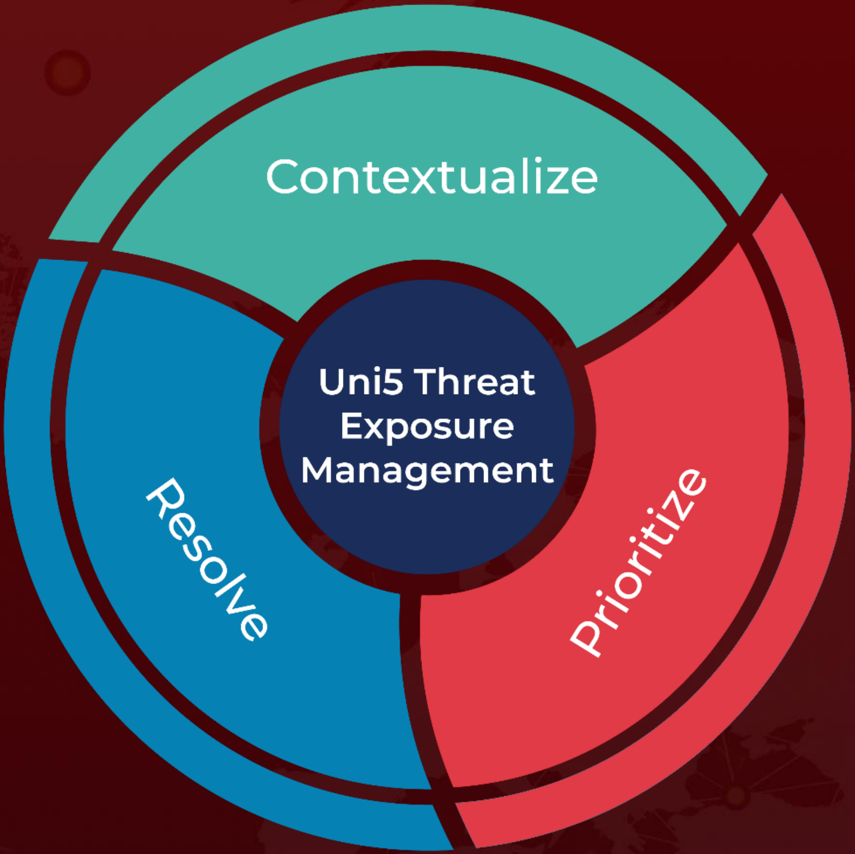
https://www.rcesecurity.com/2023/07/patch-diffing-cve-2023-28121-to-compromise-a-woocommerce/

https://github.com/gbrsh/CVE-2023-28121

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 18, 2023 • 7:00 AM

More at www.hivepro.com