Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

LiteSpeed Cache Plugin Vulnerability Affects Over 5 Million Websites

Date of Publication	Admiralty Code	TA Number
August 22, 2024	A1	TA2024322

Summary

First Seen: August 2024
Affected Products: WordPress LiteSpeed Cache plugin
Impact: A critical vulnerability has been discovered in the LiteSpeed Cache WordPress plugin, identified as CVE-2024-28000. This flaw could allow attackers to take control of millions of websites by creating rogue admin accounts. The vulnerability, classified as an unauthenticated privilege escalation, is rooted in the plugin's user simulation feature, which can be exploited by threat actors to escalate their privileges and gain unauthorized access to a website's administrative functions.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-28000	WordPress LiteSpeed Cache Privilege Escalation Vulnerability	WordPress LiteSpeed Cache plugin	✗	✗	✓

Vulnerability Details

#1 A critical vulnerability, identified as CVE-2024-28000, has been discovered in the LiteSpeed Cache WordPress plugin. This flaw poses a severe threat, potentially allowing attackers to take control of millions of websites by creating rogue administrator accounts. The vulnerability is classified as an unauthenticated privilege escalation, originating from a weak hash check in the plugin's user simulation feature.

#2 The LiteSpeed Cache plugin, a popular optimization tool used by WordPress sites for enhanced performance, fails to adequately restrict its role simulation functionality. This oversight allows unauthenticated visitors to escalate their privileges to the Administrator level. Specifically, users can set their current ID to that of an administrator, enabling attackers to spoof their user ID and create a new account with administrator privileges. All versions of the plugin up to 6.3.0.1 are affected.

#3 In environments where the plugin's crawler feature is disabled, the vulnerability might not be exploitable. However, it's important to note that this plugin has been a target for attackers in the past. Earlier this year, an unauthenticated cross-site scripting (XSS) flaw, identified as CVE-2023-40000, was exploited by attackers to create rogue administrator accounts and gain control of vulnerable websites.

#4 The exploitation of CVE-2024-28000 could result in a complete takeover of the affected sites, allowing attackers to manipulate content, steal sensitive information, and potentially use the compromised sites as launchpads for further attacks. Website administrators are strongly advised to promptly update the LiteSpeed Cache plugin and reassess their site's security measures to mitigate the risk of exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28000	WordPress LiteSpeed Cache Versions from 1.9 through 6.3.0.1.	cpe:2.3:a:litespeed:cache_plugin:*:*:*:*:*:*:*:*	CWE-266

Recommendations

Keep Plugins Updated: Ensure that all WordPress plugins, including LiteSpeed Cache plugin, are regularly updated to the latest versions to patch known vulnerabilities.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation
T1136 Create Account			

Patch Details

Website administrators should promptly update LiteSpeed Cache WordPress plugin to version 6.4 to ensure that their sites are protected against the vulnerability.

Link: https://wordpress.org/plugins/litespeed-cache/

References

https://patchstack.com/articles/critical-privilege-escalation-in-litespeed-cache-plugin-affecting-5-million-sites

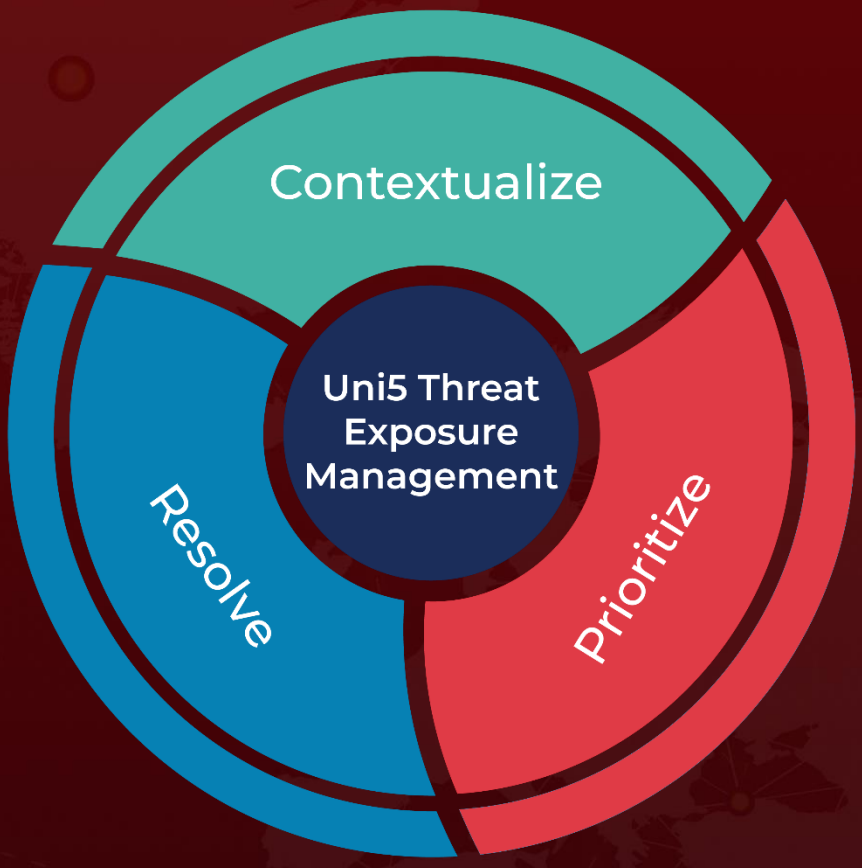
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/litespeed-cache/litespeed-cache-6301-unauthenticated-privilege-escalation

https://hivepro.com/threat-advisory/hackers-exploit-litespeed-cache-for-wordpress-site-takeover/

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

August 22, 2024 • 7:00 AM

More at www.hivepro.com