Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Hackers Exploit LiteSpeed Cache for WordPress Site Takeover

Date of Publication	Admiralty Code	TA Number
May 9, 2024	A1	TA2024179

Summary

First Seen: February 27, 2023
Affected Platform: WordPress LiteSpeed Cache Plugin
Impact: The vulnerability in LiteSpeed Cache allows attackers to inject malicious code into WordPress sites, gaining administrator access. This can lead to website takeover, data theft, and malicious activities. With millions of affected users, the impact is significant, urging immediate updates and security measures.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-40000	WordPress LiteSpeed Cache Plugin Cross Site Scripting Vulnerability	WordPress LiteSpeed Cache Plugin	✗	✗	✓

Vulnerability Details

#1

LiteSpeed Cache, a popular WordPress plugin, has a high-severity vulnerability that hackers are increasingly exploiting. This flaw, identified as CVE-2023-40000, allows unauthenticated cross-site scripting attacks. Attackers inject malicious JavaScript code through the plugin into WordPress files, enabling them to create new administrator accounts and gain complete control over websites.

#2

Exploited websites can redirect users to malicious sites, serve harmful ads, or steal sensitive data. The vulnerability affects LiteSpeed Cache versions up to 5.7.0.1, with the recommended solution being an update to version 6.2.0.1, which is immune to the flaw.

#3

LiteSpeed Cache has over five million users, with approximately two million using the outdated, vulnerable version. Users are advised to update their plugins promptly, uninstall unused plugins, and remove suspicious files and folders. Those concerned about being targeted should search their database for suspicious strings, particularly in the "litespeed[.]admin_display[.]messages" option.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-40000	WordPress LiteSpeed Cache Plugin versions prior 5.7.0.1	cpe:2.3:a:litespeed_technologies:litespeed_cache_plugin:*:*:*:*:*:*:*:*	CWE-79

Recommendations

Update LiteSpeed Cache Plugin: Ensure that the LiteSpeed Cache plugin for WordPress is updated to the latest patched version (currently version 6.2.0.1). Regularly check for plugin updates and apply them promptly to mitigate known vulnerabilities.

Review Installed Plugins: Conduct a thorough review of all installed plugins on your WordPress site. Remove any unnecessary or outdated plugins, as they may introduce security risks. Only use plugins from reputable sources and keep them updated.

Monitor User Accounts: Keep an eye on user accounts, especially admin-level accounts. Remove any suspicious users, such as "wpsupp-user" or "wp-configuser", and change passwords regularly to prevent unauthorized access.

Implement Input Validation and Sanitization: Incorporate robust input validation and sanitization mechanisms into your web applications to prevent cross-site scripting (XSS) attacks. Validate and sanitize user input before rendering it on web pages to ensure that malicious scripts cannot be injected and executed.

Implement Web Application Firewalls (WAF): Deploy a web application firewall (WAF) to provide an additional layer of defense against common web-based attacks, including XSS attacks. Configure the WAF to detect and block malicious requests before they reach your web application.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0042 Resource Development	TA0003 Persistence
TA0001 Initial Access	T1588.006 Vulnerabilities	T1136 Create Account	T1059.007 JavaScript
T1068 Exploitation for Privilege Escalation	T1059 Command and Scripting Interpreter	T1588.005 Exploits	T1588 Obtain Capabilities
T1189 Drive-by Compromise			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//dns[.]startservicefounds[.]com/service/f[.]php , hxxps[:]//api[.]startservicefounds[.]com, hxxps[:]//cache[.]cloudswiftcdn[.]com
IPv4	45.150.67[.]235

Patch Details

Update LiteSpeed Cache plugin to the latest version 6.2.0.1 or above

https://wpscan.com/vulnerability/dd9054cc-1259-427d-a4ad-1875b7b2b3b4/

References

https://wpscan.com/blog/surge-of-javascript-malware-in-sites-with-vulnerable-versions-of-litespeed-cache-plugin/

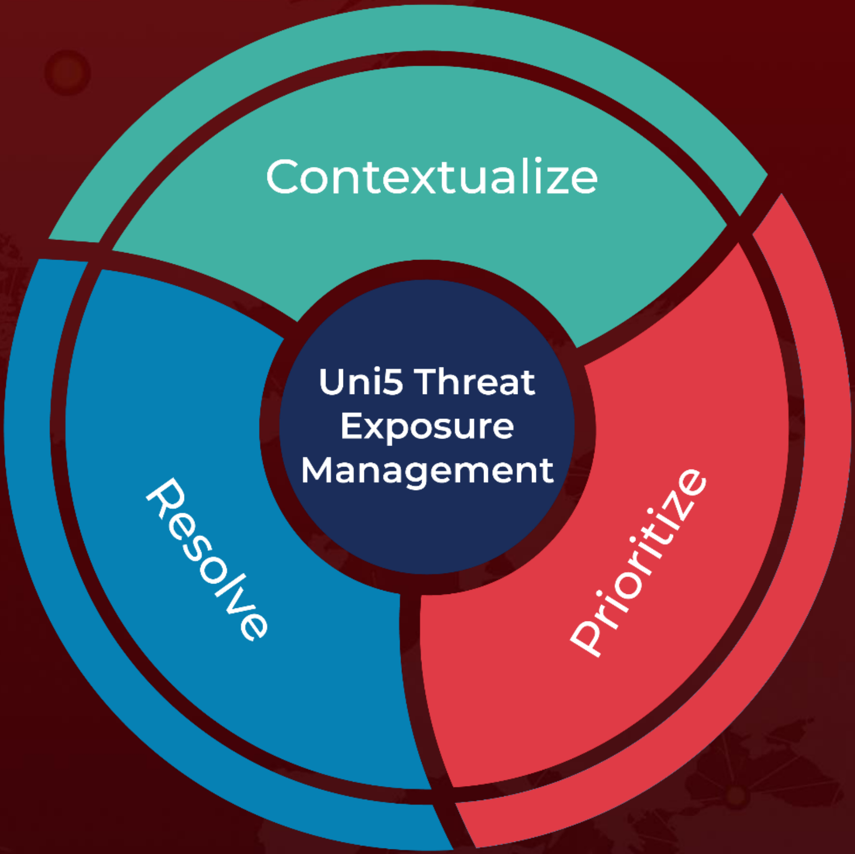
https://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-5-7-unauthenticated-site-wide-stored-xss-vulnerability?_s_id=cve

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

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

May 9, 2024 • 6:30 AM

More at www.hivepro.com