Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Vulnerability in LiteSpeed Cache Plugin Allows Website Takeover

Date of Publication	Admiralty Code	TA Number
September 10, 2024	A1	TA2024348

Summary

First Seen: 22 August 2024
Affected Products: WordPress LiteSpeed Cache plugin
Impact: A critical vulnerability, CVE-2024-44000, has been identified in the LiteSpeed Cache plugin, which is used by over 6 million WordPress sites. This flaw permits unauthorized users to gain control over any user account. The issue arises from the plugin's potential to erroneously log sensitive data, such as login cookies, in a debug log file after a login attempt.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-44000	WordPress LiteSpeed Cache Plugin Information Disclosure Vulnerability	WordPress LiteSpeed Cache plugin	✗	✗	✓

Vulnerability Details

#1 A critical vulnerability, identified as CVE-2024-44000, has been discovered in the LiteSpeed Cache plugin for WordPress. This flaw could enable attackers to gain unauthorized authentication access to any logged-in user's account, and potentially escalate privileges to an Administrator role. Once an attacker achieves Administrator access, they could upload and install malicious plugins, compromising the affected site.

#2 The vulnerability in the LiteSpeed Cache plugin stems from an HTTP response headers leak in the plugin's debug log file. Specifically, the "Set-Cookie" header, which is exposed after a login request, allows unauthenticated visitors to access sensitive cookies and potentially take control of affected WordPress installations.

#3 The problem is in the ended function, which logs all HTTP headers, including Set-Cookie, by calling self::debug() with data from headers_list(). This happens when send_headers_force is triggered during the init hook. If "Log Cookies" is turned on, it makes user cookies more visible in the debug log, raising the risk of exploitation.

#4 To mitigate this risk, update to LiteSpeed Cache plugin version 6.5.0.1, which addresses the vulnerability. Users who have previously activated the debug log feature should immediately check for and remove any residual debug log files to prevent potential attacks. Additionally, a proof-of-concept (PoC) is now available, increasing the likelihood of exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-44000	WordPress LiteSpeed Cache Plugin Versions Prior to 6.5.0.1	cpe:2.3:a:litespeed_cache_plugin:litespeed_cache_plugin:*:*:*:*:*:*:*	CWE-200

Recommendations

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

Securing Debug Log: Developers are advised to store debug logs in secure files with randomized names and use .htaccess rules to block direct access. Proper management of debug logs is essential to maintain security. Additionally, ensure that the debug log feature in the LiteSpeed Cache plugin is disabled and that the /wp-content/debug.log file has been deleted to prevent unauthorized access.

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.

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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0004 Privilege Escalation	TA0006 Credential Access
T1588 Obtain Capabilities	T1588.005 Exploits	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation
T1539 Steal Web Session Cookie	T1190 Exploit Public-Facing Application		

Patch Details

Website administrators should promptly update LiteSpeed Cache WordPress plugin to version 6.5.0.1 to ensure that their sites are protected against the vulnerability.

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

References

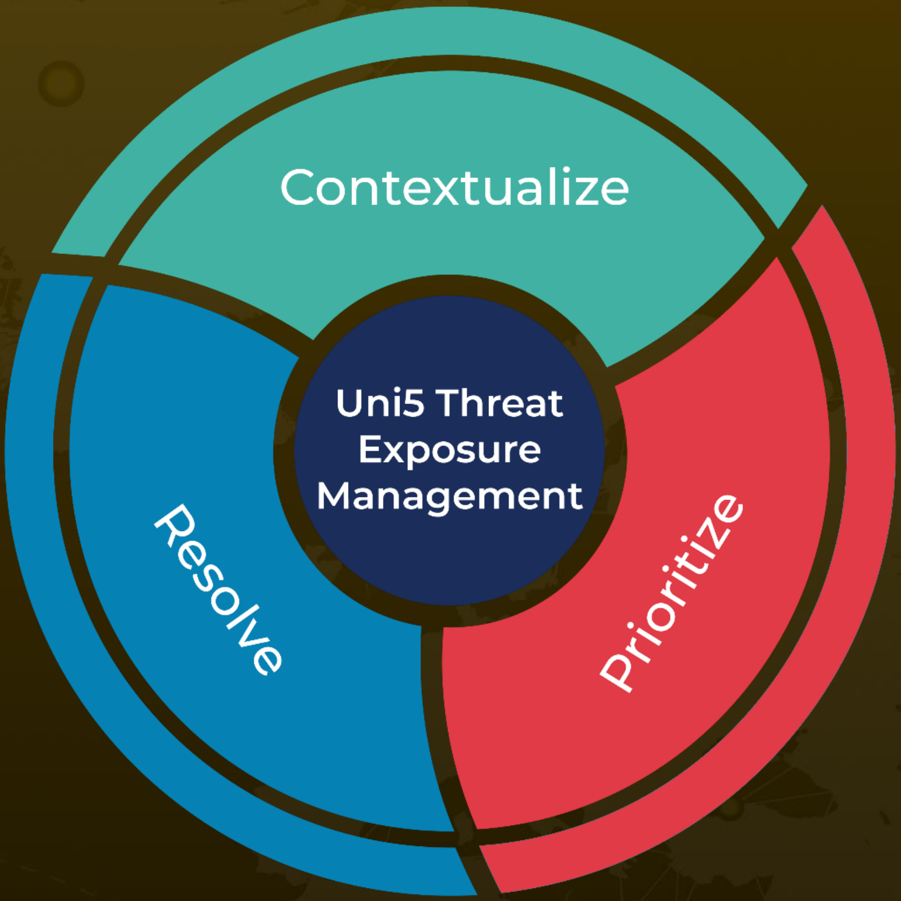
https://patchstack.com/articles/critical-account-takeover-vulnerability-patched-in-litespeed-cache-plugin/

https://github.com/gbrsh/CVE-2024-44000

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

September 10, 2024 • 7:30 AM

More at www.hivepro.com