Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

LayerSlider WordPress Plugin Flaw Impacts Over 1 Million Sites

Date of Publication	Admiralty Code	TA Number
April 4, 2024	A1	TA2024128

Summary

Discovered On: March 2024
Affected Products: LayerSlider Plugin
Impact: The discovery of a significant security vulnerability (CVE-2024-2879) in the LayerSlider plugin for WordPress, which is utilized by over a million websites, poses a serious threat. This vulnerability could potentially be exploited by malicious actors to gain unauthorized access to sensitive data stored in databases.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-2879	WordPress LayerSlider SQL Injection Vulnerability	LayerSlider Plugin	☒	☒	✓

Vulnerability Details

#1 The LayerSlider plugin for WordPress, utilized by over a million websites, has been identified as having a significant security vulnerability (CVE-2024-2879). This vulnerability exposes the plugin to unauthenticated SQL injection attacks, posing a risk of sensitive data theft from affected databases.

#2 LayerSlider is a combined graphic design programme, digital visual effects application, and visual online content editor. Users may create animations and rich content for their websites with LayerSlider.

#3 The vulnerability in the LayerSlider plugin arises from insecure handling of SQL queries, specifically in the ls_get_popup_markup() function. When the id parameter is provided and not validated as a number, it's directly passed to the find() function without proper sanitization. This omission of sanitization means that the WHERE statement in the SQL query is constructed without using the wpdb prepare() function provided by WordPress to parameterize and escape SQL queries for safe execution.

#4 Although union-based SQL injection may not be viable in this context, an attacker could potentially exploit the vulnerability using a time-based blind approach. By observing variations in response times, the attacker can extract sensitive information from the database.

#5 Versions 7.9.11 through 7.10.0 of the LayerSlider plugin are susceptible to the SQL injection vulnerability (CVE-2024-2879), posing a significant risk to WordPress sites. Exploitation of this vulnerability could lead to unauthorized access to sensitive data, such as password hashes stored in the site's database.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-2879	LayerSlider Version 7.9.11 – 7.10.0	cpe:2.3:a:layerslider_plugin:layerslider_plugin:7.9.11:*:*:*:*:*:*:* cpe:2.3:a:layerslider_plugin:layerslider_plugin:7.10.0:*:*:*:*:*:*:*	CWE-89

Recommendations

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

Deactivate Dormant Accounts: Disable any unused or dormant user accounts that could serve as potential entry points for attackers.

Disable Unnecessary Plugins: Deactivate or uninstall any plugins that are not essential for the website's functionality to reduce the attack surface.

Implement a Web Application Firewall (WAF): WAFs play a crucial role in detecting and mitigating SQL injection attacks. They analyze HTTP requests in real-time, looking for suspicious patterns and signatures commonly associated with SQL injection attempts. By monitoring the behavior of web applications, WAFs can identify abnormal activities indicative of an attack.

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	TA0006 Credential Access
TA0007 Discovery	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1555 Credentials from Password Stores	T1505 Server Software Component		

Patch Details

Website administrators should promptly update the LayerSlider plugin to version 7.10.1 to ensure that their sites are protected against the SQL injection vulnerability.

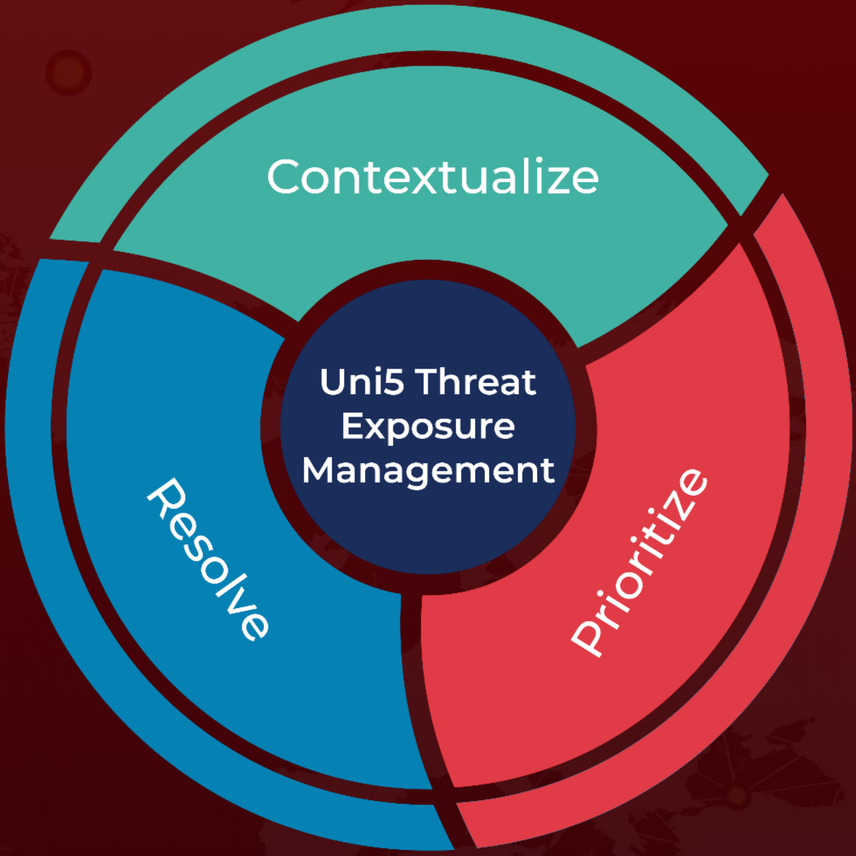
References

https://www.wordfence.com/blog/2024/04/5500-bounty-awarded-for-unauthenticated-sql-injection-vulnerability-patched-in-layerslider-wordpress-plugin/

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

April 4, 2024 • 5:50 AM

More at www.hivepro.com