CYBER ADVISORY

TLP:CLEAR
12 March 2024

WordPress Ultimate Member Plugin Vulnerability

CVE-2024-2123 | Ultimate Member | XSS | High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2024-2123.[1] The vulnerability affects WordPress Plugin Ultimate Member version 2.8.3 and below.[2] Exploitation of the Stored Cross-Site Scripting (XSS) vulnerability may allow an unauthenticated attacker to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.[3,4]

The Cal-CSIC recommends upgrading to WordPress Ultimate Member version 2.8.4 or newer as soon as possible.

For further information on applying upgrades, please refer to WordPress Ultimate Member.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Security Week; "Ultimate Member Plugin Flaw Exposes 100,000 WordPress Sites to Attacks;" https://www.securityweek.com/ultimate-member-plugin-flaw-exposes-100000-wordpress-sites-to-attacks/; accessed 12 March 2024

[2] Wordfence; "Unauthenticated Stored XSS Vulnerability Patched in Ultimate Member WordPress Plugin;" https://www.wordfence.com/blog/2024/03/unauthenticated-stored-xss-vulnerability-patched-in-ultimate-member-wordpress-plugin/; accessed 12 March 2024

[3] Wordfence Intelligence; "Ultimate Member <= 2.8.3 - Unauthenticated Stored Cross-Site Scripting;" https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ultimate-member/ultimate-member-283-unauthenticated-stored-cross-site-scripting; accessed 12 March 2024

[4] The Hacker News; "Malware Campaign Exploits Popup Builder WordPress Plugin to Infect 3,900+ Sites);" https://thehackernews.com/2024/03/malware-campaign-exploits-popup-builder.html; accessed 12 March 2024