CYBER ADVISORY

TLP:CLEAR

18 March 2024

WordPress miniOrange Vulnerability

CVE-2024-2172 | miniOrange | WordPress | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2024-2172.[1] The vulnerability affects WordPress users of miniOrange's Malware Scanner plugin versions 4.7.2 and below and Web Application Firewall plugin versions 2.1.1 and below.[2] Exploitation of the vulnerability may allow an unauthenticated attacker to arbitrarily update any user's password and escalate privileges to that of an administrator, potentially leading to a complete compromise of the site. [3]

The Cal-CSIC recommends to immediately delete miniOrange's Malware Scanner and the Web Application Firewall plugins from all websites and utilize an alternate plugin.

For further information on Word Press miniOrange permanent closure of plugins, please refer to WordPress Plugins.

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] National Vulnerability Database; "CVE-2024-2172 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-2172; accessed 18 March 2024
[2] The Hacker News; "WordPress Admins Urged to Remove miniOrange Plugins Due to Critical Flaw;" https://thehackernews.com/2024/03/wordpress-admins-urged-to-remove.html; accessed 18 March 2024
[3] Wordfence; "Critical Vulnerability Remains Unpatched in Two Permanently Closed MiniOrange WordPress Plugins – $1,250 Bounty Awarded;" https://www.wordfence.com/blog/2024/03/critical-vulnerability-remains-unpatched-in-two-permanently-closed-miniorange-wordpress-plugins-1250-bounty-awarded/; accessed 18 March 2024