



CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

TLP: CLEAR
20 August 2024

GiveWP Vulnerability

CVE-2024-5932

GiveWP

Word Press

Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-5932, with a reported CVSS v3 rating of 10.0.¹ The vulnerability affects the WordPress plugin GiveWP in all versions up to, and including, 3.14.1.² Exploitation of the Hypertext Preprocessor (PHP) Object Injection vulnerability may allow an unauthenticated attacker to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code remotely, and to delete arbitrary files.³

The Cal-CSIC recommends immediately upgrading to GiveWP version 3.14.2 or newer.

For further information on applying upgrades please refer to [GiveWP](#).

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.

CAL-CSIC-202408-004

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP: CLEAR

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

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-2024-5932 Detail;" <https://nvd.nist.gov/vuln/detail/cve-2024-5932>; accessed 20 August 2024

² Security Week; "Critical Flaw in Donation Plugin Exposed 100,000 WordPress Sites to Takeover" <https://www.securityweek.com/critical-flaw-in-donation-plugin-exposed-100000-wordpress-sites-to-takeover/>; accessed 20 August 2024

³ WordFence; "GiveWP – Donation Plugin and Fundraising Platform <= 3.14.1 - Unauthenticated PHP Object Injection to Remote Code Execution" <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/give/givewp-donation-plugin-and-fundraising-platform-3141-unauthenticated-php-object-injection-to-remote-code-execution>; accessed 20 August 2024

CAL-CSIC-202408-004

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR