CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
23 December 2024

Code Injection in Craft's Content Management System leads to RCE

CVE-2024-56145 | Craft CMS | RCE | register_argc_argv

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability, CVE-2024-56145, existing in Craft's Content Management System (CMS), a widely used PHP-based CMS existing in versions prior to 5.5.2, 4.13.2, and 3.9.14.[1] Craft CMS is a flexible tool designed for building custom websites and digital experiences.[2] The potential impact of exploitation is that an attacker could perform remote code execution (RCE) on vulnerable versions if one's php.ini configuration has register_argc_argv enabled. There is currently a proof-of-concept established and is publicly available on GitHub, however there are no reported cases of this vulnerability being actively exploited.[3]

The Cal-CSIC recommends immediately updating to the latest Craft CMS version 5.5.2, 4.13.2 and 3.9.14

For further information on applying updates please refer to Craft's release documentation.

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 here.

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.

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] GitHub; "Potential RCE when PHP `register_argc_argv` config setting is enabled" https://github.com/craftcms/cms/security/advisories/GHSA-2p6p-9rc9-62j9; accessed 23 December 2024
[2] Craft; "Craft empowers the entire creative process." https://craftcms.com/; accessed 23 December 2024
[3] GitHub; "CVE-2024-56145" https://github.com/Chocapikk/CVE-2024-56145; accessed 23 December 2024