CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
12 March 2025

PHP-CGI Critical Vulnerability Update

PHP | CVE-2024-4577 | Active Exploitation | RCE Vulnerability

In June 2024, the California Cybersecurity Integration Center (Cal-CSIC) became aware of a critical vulnerability (CVE-2024-4577) affecting Hypertext Preprocessor (PHP) in our previous Cyber Advisory (serial number CAL-CSIC-202406-002). In PHP versions **8.1-8.1.29** (*excluding* 8.1.29), **8.2-8.2.20** (*excluding* 8.2.20), and **8.3-8.3.8** (*excluding* 8.3.8), when using Apache and PHP-CGI on Windows, a "Best-fit" behavior in character encoding can allow malicious users to inject options into the PHP binary, potentially exposing script source code or executing arbitrary PHP code.

Recently, researchers from GreyNoise Intelligence have warned of a significant rise in exploitation attempts observed in their Global Observation's Grid (GOG) honeypot, indicating mass exploitation of the vulnerability[1]. Additionally, Cisco Talos published a report on a sophisticated campaign targeting Japanese organizations through the vulnerability (CVE-2024-4577) since as early as January 2025 [2]. Ransomware groups have previously used this vulnerability to deploy web shells and encrypt victim's systems[3].

The Cal-CSIC recommends immediately upgrading to PHP to the newest version.

For further information on applying upgrades please refer to PHP 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.

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.

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.
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] Greynoise; “GreyNoise Detects Mass Exploitation of Critical PHP-CGI Vulnerability (CVE-2024-4577), Signaling Broad Campaign”; https://www.greynoise.io/blog/mass-exploitation-critical-php-cgi-vulnerability-cve-2024-4577; accessed 12 March 2025.

[2] Cisco Talos; “Unmasking the new persistent attacks on Japan”; https://blog.talosintelligence.com/new-persistent-attacks-japan/; accessed 12 March 12, 2025.

[3] BleepingComputer; “Critical PHP RCE vulnerability mass exploited in new attacks”; https://www.bleepingcomputer.com/news/security/critical-php-rce-vulnerability-mass-exploited-in-new-attacks/; accessed 12 March 2025.

CAL-CSIC-202503-002

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