CYBER ADVISORY

TLP:CLEAR
10 June 2024

PHP-CGI Argument Injection Vulnerability

CVE-2024-4577 | PHP | Argument Injection | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability under active exploit known as CVE-2024-4577.[1] The vulnerability affects Hypertext Preprocessor (PHP) when PHP is running with Common Gateway Interface (CGI) mode enabled on the Windows operating system.[2] The vulnerability lies in version branches 8.3 prior to 8.3.8, 8.2 prior to 8.2.20, and 8.1 prior to 8.1.29. Exploitation of the vulnerability may allow an attacker to execute arbitrary code on remote PHP servers through an argument injection attack.[3,4]

The Cal-CSIC recommends to immediately upgrade to PHP versions of 8.1.29, 8.2.20 or 8.3.8.

For further information on applying PHP upgrades please refer to PHP 8 Change Log.

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] Ars Technica "Nasty bug with very simple exploit hits PHP just in time for the weekend;" https://arstechnica.com/security/2024/06/php-vulnerability-allows-attackers-to-run-malicious-code-on-windows-servers/; accessed 10 June 2024
[2] Devcore; "Security Alert: CVE-2024-4577 - PHP CGI Argument Injection Vulnerability;" https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/; accessed 10 June 2024
[3] Tenable; "CVE-2024-4577: Proof of Concept Available for PHP-CGI Argument Injection Vulnerability" https://www.tenable.com/blog/cve-2024-4577-proof-of-concept-available-for-php-cgi-argument-injection-vulnerability; accessed 10 June 2024
[4] Imperva; "Imperva Protects Against Critical PHP Vulnerability CVE-2024-4577" https://www.imperva.com/blog/imperva-protects-against-critical-php-vulnerability-cve-2024-4577/; accessed 10 June 2024