

CVE-2024-4577

PHP Group PHP-CGI OS Command Injection Vulnerability

Exigent
CISA KEV since Jun 12, 2024
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

EVRS 94/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE JUL 3, 2024 KEV since 2024 · listed over a year
--	--	---	---

Signals behind the score

☒ counted in the score
 ☐ not counted
 evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.

Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
php	$\geq 8.1.0 < 8.1.29$ $\geq 8.2.0 < 8.2.20$ $\geq 8.3.0 < 8.3.8$	8.1.29 · 8.2.20 · 8.3.8	NVD
windows	—	no fixed version listed	NVD
fedora	39 40	no fixed version listed	NVD

Sources

Vendor guidance	github.com/rapid7/metasploit-framework/pull/19247	php.net	php.net/ChangeLog-8.php#
NVD	nvd.nist.gov/vuln/detail/CVE-2024-4577	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-44188	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-4577

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.