

CVE-2012-1823

PHP-CGI Query String Parameter Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · 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	No known ransomware campaign association	☐ 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 9 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
php	< 5.3.12 ≥ 5.4.0 < 5.4.2	5.3.12 · 5.4.2	NVD
application stack	2.0	no fixed version listed	NVD
gluster storage server for on-premise	2.0	no fixed version listed	NVD
storage	2.0	no fixed version listed	NVD
storage for public cloud	2.0	no fixed version listed	NVD
fedora	39 40	no fixed version listed	NVD
debian linux	6.0	no fixed version listed	NVD
hp-ux	b.11.23 b.11.31	no fixed version listed	NVD

Sources

Vendor guidance bugs.php.net/bug.php?id=61910

Additional guidance lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/PKGTQU0A2NTZ3RXN22CSAUJPIRUYRB4B/cisa.gov/known-exploited-vulnerabilities-catalog

NVD nvd.nist.gov/vuln/detail/CVE-2012-1823

CISA KEV

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2012-1833

Current data evulnable.com/vulnerability-management/cve/CVE-2012-1823

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