

CVE-2017-9841

PHPUnit Command Injection Vulnerability

Exigent

CISA KEV since Feb 15, 2022

Actively exploited

Util/PHP/eval-stdin.php in PHPUnit before 4.8.28 and 5.x before 5.6.3 allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a "<?php " substring, as demonstrated by an attack on a site with an exposed /vendor folder, i.e., external access to the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php URI.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE Aug 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
phpunit/phpunit	≥ 4.8.19, < 4.8.28	4.8.28	GitHub
phpunit/phpunit	≥ 5.0.10, < 5.6.3	5.6.3	GitHub
phpunit	≤ 4.8.27 ≥ 5.0.0 < 5.6.3	no fixed version listed	NVD
communications diameter signaling router	≥ 8.0.0 ≤ 8.5.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/sebastianbergmann/phpunit/commit/284a69fb88a2d0845d23f42974a583d8f59bf5a5	Additional guidance	security.gentoo.org/glsa/201711-15
NVD	nvd.nist.gov/vuln/detail/CVE-2017-9841	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-r7c9-c69m-rph8	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-1528
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-9841		

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