



CVE-2017-9841

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-9841
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-27 17:29:00 UTC
Updated	2026-04-21 18:00:56 UTC
Description	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

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.942100000 probability, percentile 0.999230000 (date 2026-04-22)

CISA KEV: Listed on 2022-02-15; due 2022-08-15; ransomware use Unknown

Problem Types: CWE-94 | n/a | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

CISA Known Exploited Vulnerability

Vendor	PHPUnit
Product	PHPUnit
Name	PHPUnit Command Injection Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-9841

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Communications Diameter Signaling Router	All	All	All	All
Application	Phpunit Project	Phpunit	All	All	All	All
Application	Phpunit Project	Phpunit	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

Oracle Critical Patch Update Advisory - October 2021

www.cisa.gov/known-exploited-vulnerabilities-catalog

PHPUnit CVE-2017-9841 Arbitrary Code Execution Vulnerability

Fix insulated tests with phpdbg by nicolas-grekas · Pull Request #1956 · sebastianbergmann/phpunit · GitHub

MediaWiki Multiple Flaws Let Remote Users Modify Data, Obtain Potentially Sensitive Information, and Conduct Cross-Site Scripting Attacks

PHPUnit: Remote code execution (GLSA 201711-15) — Gentoo security

Correct fix for #1956 · sebastianbergmann/phpunit@284a69f · GitHub

CVE-2017-9841 RCE vulnerability in phpunit

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-02-15T00:00:00.000Z	CVE-2017-9841 added to CISA KEV

Legacy QID Mappings

710371 Gentoo Linux Hypertext Preprocessor (PHP) Unit Remote code execution Vulnerability (GLSA 201711-15)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report