



# Global buffer over-read in mb\_convert\_encoding() with attacker-supplied encoding

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

## Summary

<b>CVE</b>	CVE-2026-6104
<b>State</b>	PUBLISHED
<b>Assigner</b>	php
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-10 06:16:07 UTC
<b>Updated</b>	2026-05-10 06:16:07 UTC

**Description** In PHP versions 8.4.\* before 8.4.21 and 8.5.\* before 8.5.6, when an encoding name containing an embedded NUL byte is p

## Risk And Classification

**Primary CVSS:** v4.0 6.3 MEDIUM from security@php.net

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:L/SI:N/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:M/U:Amber

**Problem Types:** CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	security@php.net	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:L/SI:N/SA:L/E:X/C...
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:L/SI:N/SA:L/RE:M/...

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

Low

Sub Conf.

Low

Sub Integrity

None

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:L/SI:N/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:M/U:Amber

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">PHP Group</a>	<a href="#">PHP</a>	affected 8.4.* 8.4.21 semver	Not specified
CNA	<a href="#">PHP Group</a>	<a href="#">PHP</a>	affected 8.5.* 8.5.6 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="https://github.com/php/php-src/security/advisories/GHSA-74r9-qxhc-fx53">github.com/php/php-src/security/advisories/GHSA-74r9-qxhc-fx53</a>	<a href="mailto:security@php.net">security@php.net</a>	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Akshay Jain (en)

**CNA:** Ilija Tovilo (en)

There are currently no legacy QID mappings associated with this CVE.

© 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)