



Use-After-Free in SOAP using Apache map

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-6722
State	PUBLISHED
Assigner	php
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-10 05:16:11 UTC
Updated	2026-05-10 05:16:11 UTC
Description	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, the SOAP extension's c

Risk And Classification

Primary CVSS: v4.0 9.5 CRITICAL from security@php.net

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:Y/R:X/V:X/RE:M/U:R
ed

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
4.0	security@php.net	Secondary	9.5	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:Y/R:X/V:X/RE:M/U:R
4.0	CNA	CVSS	9.5	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/AU:Y

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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:Y/R:X/V:X/RE:M/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PHP Group	PHP	affected 8.2.* 8.2.31 semver	Not specified
CNA	PHP Group	PHP	affected 8.3.* 8.3.31 semver	Not specified
CNA	PHP Group	PHP	affected 8.4.* 8.4.21 semver	Not specified
CNA	PHP Group	PHP	affected 8.5.* 8.5.6 semver	Not specified

References

Reference	Source	Link	Tags
github.com/php/php-src/security/advisories/GHSA-85c2-q967-79q5	security@php.net	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: [brettgervasoni \(en\)](#)

CNA: [Ilija Tovilo \(en\)](#)

CNA: [Nora Dossche \(en\)](#)

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

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