ALVD-2026-316

ID alternative: CVE-2026-6722

9.5 | KRITIK

PËRSHKRIM

PHP ka një cenueshmëri use-after-free në mekanizmin e përpunimit të objekteve të extension-it SOAP. Kur një node apache:Map përmban duplicate keys, objekti i parë mund të lirohet nga memory, ndërsa një stale pointer ndaj tij vazhdon të përdoret.

Një sulmues që kontrollon body-n e SOAP request mund ta shfrytëzojë këtë cenueshmëri për remote code execution.

MASAT E REKOMANDUARA

Rekomandohet përditësimi i menjëhershëm i PHP në versionin 8.2.31 ose më të ri për degën 8.2.x, 8.3.31 ose më të ri për degën 8.3.x, 8.4.21 ose më të ri për degën 8.4.x dhe 8.5.6 ose më të ri për degën 8.5.x.

Pas përditësimit, shërbimet PHP dhe endpoint-et SOAP duhet të rinisen dhe të testohen.

KRITIKALITETI
CVSS Base Score: 9.5 (Kritik)
Versioni CVSS: 4.0

PUBLISHED
10.05.2026

VENDOR
PHP Group PHP

PRODUCT
PHP

VERSION
Nga 8.2.0 deri 8.2.30
Nga 8.3.0 deri 8.3.30
Nga 8.4.0 deri 8.4.20
Nga 8.5.0 deri 8.5.5

PRODUKTI I PREKUR

PRODHUESI	PRODUKTI	VERSIONI	ZGJIDHUR	PUBLIKUAR
PHP Group PHP	PHP	Nga 8.2.0 deri 8.2.30 Nga 8.3.0 deri 8.3.30 Nga 8.4.0 deri 8.4.20 Nga 8.5.0 deri 8.5.5	8.2.31 8.3.31 8.4.21 8.5.6	10.05.2026

REFERENCA

- https://github.com/php/php-src/security/advisories/GHSA-85c2-q967-79q5
- https://www.cve.org/CVERecord?id=CVE-2026-6722