OpenVault

Security Advisory: PHP Vulnerabilities CVE-2026-109618 and CVE-2026-109619

Oct 23, 2026

Overview

On October 21, 2026, The PHP Foundation announced security releases for two critical vulnerabilities in PHP. The flaws, tracked as CVE-2026-109618 and CVE-2026-109619, affect PHP web server deployments and could potentially lead to remote code execution (RCE) on the affected systems.

Vulnerability details

Field	CVE-2026-109618	CVE-2026-109619
Publicly reported	Oct 21, 2026	Oct 21, 2026
Type	RCE via out-of-memory (OOM) corruption	RCE via stale global state
Severity	CVSS v4.0 9.2 (Critical)	CVSS v4.0 9.2 (Critical)
Fixed in	PHP 8.5.12, 8.4.27, 8.3.36, and 8.2.35	PHP 8.5.12, 8.4.27, 8.3.36, and 8.2.35
References	CVE-2026-109618	CVE-2026-109619

Our evaluation

After the disclosure, our security teams reviewed the OpenVault products and supporting infrastructure.

Area	Finding	Status
OpenVault products	OpenVault products do not use PHP, and none of them are affected by these vulnerabilities.	Not affected
Public web content	A few of our blogs and public static pages are hosted on PHP web servers. These have been updated to the patched PHP versions.	Patched
Internal services	A few of our internal services use the PHP web server. These are not reachable from the public internet, which limits exposure. However, we have updated to the patched version.	Patched

Customer impact and required action

No impact on customer data or on the functionality of OpenVault products has been identified, and **no action is required on the part of our customers**. We have found no evidence of exploitation in our environment.

OpenVault continuously monitors security advisories and evaluates potential vulnerabilities in order to safeguard the security of its services and the integrity of customer data. We will promptly notify you of any relevant findings or changes.

Contact

For questions, please contact our security team at security@openvault.com.