

Two Critical Remote Code Execution Vulnerabilities in PHP (CVE-2026-109618 & CVE-2026-109619)

Oct 21, 2026

☐ WHITE

[View Alert](#)

UPDATE: On October 21, 2026, Health-ISAC created a dedicated [channel](#) regarding the release of [patches](#) for the two critical remote code execution vulnerabilities affecting PHP infrastructure.

On October 20, 2026, the PHP development team issued a notice advising administrators to prepare for emergency security updates.

The upcoming [patches](#) address two vulnerabilities, tracked as [CVE-2026-109618](#) and [CVE-2026-109619](#), that were reportedly [leaked](#) before their scheduled disclosure. Security researchers indicate these are remote code execution flaws affecting multiple PHP versions.

Although no active exploitation has been observed, administrators are urged to apply updates promptly once official patches are released.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to the vulnerabilities.

Additional Info

Analysis:

On October 20, 2026, someone using the moniker “**petecooper**” prematurely [leaked](#) two critical remote code execution vulnerabilities in PHP Core, tracked as [CVE-2026-109618](#) and [CVE-2026-109619](#), and said the PHP team would officially disclose them on October 22.



The PHP security team and [coordinating researchers](#) have intentionally withheld full technical details, proof-of-concept exploits, and exact vulnerable code paths pending the official patch release.

The two flaws are currently rated **9.2** (Critical) under the CVSS v4.0 framework by the official PHP security team. As of this writing, no active exploitation in the wild or public exploit code has been confirmed or observed.

Current unofficial preliminary security analysis and community [disclosures](#) indicate the flaws affect multiple core PHP branches, including **versions 5, 6, 7, and 8**. Official security updates and fixes will only be issued for currently supported PHP 8 release branches. Outdated, end-of-life branches (such as PHP 5 and PHP 7) will not receive official patches from the development team. However, the PHP team will [publish](#) full details, affected versions, and fixed versions on **October 21, 2026 at 14:00 UTC**.

Meanwhile, health sector networks rely on custom web services and content management platforms. Unplanned software leaks introduce distinct operational risks across patient portals and critical clinical infrastructure environments.

Remote code execution vulnerabilities, such as these PHP flaws, complicate medical operations by threatening data integrity. Swift asset discovery and administrative oversight remain necessary to effectively protect sensitive electronic health records.

Legacy systems compound exposure because older software branches often lack ongoing maintenance. Health sector organizations' administrators must evaluate active application inventories immediately to isolate vulnerable assets before exploitation occurs.

Recommendations:

Health-ISAC provides this information to prevent the successful exploitation and disruption of your security apparatus. For more information, see [Health Industry Cybersecurity Practices \(HICP\): Managing Threats and Protecting Patients](#).

Health-ISAC recommends organizations review and assess their risk exposure to these vulnerabilities and implement the following:

- Immediately inventory all web servers and applications to identify active PHP versions across clinical networks.
- Prioritize upgrading systems running outdated legacy PHP editions to currently supported branches.
- Apply official security [updates](#) promptly upon release while monitoring vendor and advisory channels.
- Implement temporary network segmentation or isolation for internet-facing applications if immediate patching is not feasible.

Alert Id	52c94a8e
Category	Vulnerability Bulletins
References	hhs europa cyberkendra php threatlandscape cyberdaily bleepingcomputer watchtowr php 1
Tags	CVE-2026-109619, CVE-2026-109618, Remote Code Execution, PHP

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback



Download the App

Available on iOS, Android and Web



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to toc@h-isac.org

--

You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.

To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.

To view this discussion visit <https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a15efe9619-f485e434-2c5d-4eff-84d0-bc289a693eef-000000%40email.amazonses.com>.