

SN-15

CVE-2026-109618 and CVE-2026-109619

PHP2Shell Vulnerabilities

Version 1.0.0

1 Overview

This report summarizes the two PHP vulnerabilities addressed in the security updates released on October 21, 2026, and explains the rationale for the IDIS impact assessment. The assessment is based on confirmation from IDIS R&D that IDIS products and solutions do not use PHP.

IDIS products and solutions do not use PHP and are therefore not affected by the PHP2Shell vulnerabilities (CVE-2026-109618 and CVE-2026-109619). No IDIS firmware or software updates are required to address these vulnerabilities.

2 Vulnerability Details

The details and technical summaries of the vulnerabilities analyzed are as follows:

Item	CVE-2026-109618	CVE-2026-109619
Vulnerability	RCE via OOM corruption	RCE via stale global state
Cause	Partially initialized internal data may be treated as valid during out-of-memory handling.	Internal state may retain pointers to freed memory and be reused by a later request.
Type	Improper handling of exceptional conditions and memory corruption	Use After Free
Severity	Critical / CVSS v4.0 9.2	Critical / CVSS v4.0 9.2
Main impact	Unauthenticated remote code execution under applicable conditions	Unauthenticated remote code execution under applicable conditions
Fix released	October 21, 2026	October 21, 2026

PHP installations that serve web requests require assessment. These include PHP-FPM, Apache mod_php, php-cgi, FrankenPHP, and LiteSpeed. The PHP project identifies mod_php as the highest-risk configuration.

The severity ratings above apply to vulnerable PHP environments. They do not represent the risk level of IDIS products and solutions, which do not use PHP.

For reference, affected and fixed versions for external systems using PHP are listed below. The same version thresholds apply to both CVEs.

PHP branch	Affected versions	Fixed version or action
8.2	Earlier than 8.2.35	8.2.35 or later
8.3	Earlier than 8.3.36	8.3.36 or later
8.4	Earlier than 8.4.27	8.4.27 or later
8.5	Earlier than 8.5.12	8.5.12 or later
8.1 and earlier	End-of-life branches also require assessment	Upgrade to a supported branch or verify a vendor-provided fixed package.

If a distribution or long-term support vendor has backported the fixes, verify that its package addresses both CVEs rather than relying solely on the displayed PHP version number.

3 Affected Products

Affected IDIS products: None.

IDIS R&D has confirmed that **No** IDIS products, including IPCs and NVRs, or solutions, including IDIS Solution Suite(VMS), IDIS Center, WebGuard, FEN, Push use PHP.

4 Detailed Description (Rationale)

Both vulnerabilities involve memory management and request processing in the PHP runtime. CVE-2026-109618 can cause memory corruption when an out-of-memory interruption leaves internal data partially initialized and request cleanup subsequently processes that data. CVE-2026-109619 can leave internal state pointing to memory freed during a previous request, which a later request handled by the same worker may then use.

IDIS R&D has confirmed that none of the company's products or solutions use PHP. The prerequisite for executing the affected PHP code is therefore absent in the IDIS products and solutions covered by this assessment. Both CVEs are classified as "Not Affected." This conclusion is based on the absence of PHP use, rather than on temporary mitigations such as firewall rules or authentication settings.

The presence of a web interface alone does not establish whether a product uses PHP. This assessment covers IDIS products and solutions. External web applications, PHP runtimes, and third-party services separately installed or integrated by customers must be assessed according to their respective vendors' guidance.

5 Impact Assessment and Rationale by Product Family (Impact Analysis)

All assessments below are based on IDIS R&D's confirmation that none of the company's products or solutions use PHP.

Product family / solution	PHP use	Impact	Rationale
IPC	Not used	Not affected	The prerequisite for executing the affected PHP code is absent.
NVR and other IDIS products	Not used	Not affected	PHP is not used in any IDIS product.
IDIS Solution Suite	Not used	Not affected	The prerequisite for executing the affected PHP code is absent.
IDIS Center	Not used	Not affected	The prerequisite for executing the affected PHP code is absent.
WebGuard	Not used	Not affected	The prerequisite for executing the affected PHP code is absent.
FEN and Push	Not used	Not affected	The prerequisite for executing the affected PHP code is absent.
other IDIS solutions	Not used	Not affected	PHP is not used in any IDIS solution.

6 Conclusion & Recommendations

IDIS products and solutions are not affected by PHP2Shell. No IDIS firmware or software updates or suspension of functionality are required in response to these vulnerabilities.

For separately operated PHP-based servers and external integrated systems, customers should consult the relevant vendors' impact assessments and patch guidance. Apply fixed releases to affected PHP environments. If patching is delayed, consider reducing exposure through measures such as restricting external access. Configuration changes alone do not fully resolve both vulnerabilities.

Continue to follow existing security practices and regular update policies. For questions about IDIS products and solutions, contact your IDIS technical support representative.

7 References

References

- [1] PHP Security Advisory and Release Announcements, October 21, 2026
- [2] PHP Security Advisory GHSA-w8hw-w9fx-j79w
- [3] PHP Security Advisory GHSA-6wmf-4rv5-p3rp
- [4] KISA PHP Security Update Recommendation, October 21, 2026
- [5] IDIS R&D response, October 22, 2026: Confirmation that IDIS products and solutions do not use PHP

Contact Us

Additional information may be updated in this document in the future. For any questions or concerns related to this issue, please email security@idisglobal.com.

Version History

Version	Writer	Revision Date	Remarks
1.0.0	Roy Lee	Oct. 22. 2026	Initial Release