Security Advisory No. 004

Date: 27th Oct 2026

PHP2Shell vulnerabilities CVE-2026-109618 and CVE-2026-109619 in PHP

Advisory ID: PD-2026-0001
Document Version: 1.1
First published: 2026-10-27
Last updated: 2026-10-28
Status: Assessment ongoing

Advisory Title

PHP2Shell vulnerabilities CVE-2026-109618 and CVE-2026-109619 in PHP

Summary

Dynalite is aware of the recently disclosed PHP vulnerabilities identified as CVE-2026-109618 and CVE-2026-109619 (collectively referred to as "PHP2Shell").

According to information published by the PHP project, these vulnerabilities may allow remote code execution in certain affected PHP installations under specific conditions. Dynalite has assessed its product portfolio to determine potential exposure and is continuing its review of the impact on potential affected products.

Advisory CVE IDs

CVE-2026-109618
CVE-2026-109619

Affected products

The following products contain a version of PHP that has been reported as affected by CVE-2026-109618 and CVE-2026-109619. Based on Dynalite's current assessment, no verified exploitation path affecting these products has been identified. However, customers are encouraged to apply available mitigations and install updated firmware as soon as it becomes available. Dynalite is preparing firmware updates that include a supported version of the affected component.

Product	Affected Versions	Remediation
PDDEG-S	Firmware version 2.27 and earlier	Update to new firmware when available
PDTS	Firmware version 4.09 and earlier	Update to new firmware when available

At the time of publication, Dynalite has not identified additional affected products.

Details

Dynalite intends to make firmware updates available for the products listed above. Fixed firmware versions will be published in an update to this advisory.

Obtaining Software Fixes

Software fixes will be made available through the Signify Dynalite Distributor Support website. https://support.dynalite.com/support

Mitigations and Workarounds

As a precaution and in line with general good practice, Dynalite recommends the following defensive measures to minimize the risk of exploitation of the vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the public internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods such as Virtual Private Networks (VPNs).

Additional Information

This advisory reflects the information available and the status of Dynalite's assessment as of 27 October 2026. It may be updated if the ongoing validation identifies information relevant to customers.

For advisories regarding other Signify products and services refer to https://www.signify.com/global/product-security/security-advisory

Terms of use

Signify Security Advisories are subject to the terms and conditions contained in Signify underlying applicable agreements previously agreed to with Signify.