IA-2026-01: PHP2Shell Security Advisory v1.2

CVE-2026-109618 and CVE-2026-109619

Publication Date	21/10/2026	**Last Update**	23/10/2026
Current Version	1.2	**Status**	Assessment ongoing
Severity	CRITICAL	**Customer Impact**	**Temporary service unavailability and restore**

Summary

Signify is aware of the recently disclosed critical PHP vulnerabilities known as PHP2Shell. Following publication of the information, Signify initiated an assessment of its products, services, and supporting infrastructure.

Current assessment: The vast majority of Signify customer-facing products, cloud services, and supporting infrastructure assessed are not affected.

Current Status

- No evidence of the vulnerability or exploitation has been identified within Signify environments.
- The vast majority of products, services, and supporting infrastructure assessed to date are not affected.
- Telensa PLANet V2 and Interact VBI Space Analyzer were taken offline as a precaution. Telensa PLANet V2 has been patched and back online.
- The teams are currently applying patches to these systems, which are expected to return online soon.
- Signify continues to monitor official updates and relevant security intelligence as the situation develops.

Customer Impact

- As a precaution, Telensa PLANet and Interact VBI Space Analyzer were taken offline temporarily while patches are applied. Telensa PLANet V2 has been patched and back online. For Interact VBI Space Analyzer, the teams are currently applying patches. This system is expected to return online soon. Customers do not need to take any action at this time.

If the ongoing review of systems identifies any customer-relevant impact, Signify will implement appropriate measures and communicate directly with affected customers where necessary.

Actions Taken by Signify

- Activated the established vulnerability management and incident-assessment processes.
- Reviewed customer-facing products, cloud services, supporting infrastructure, and relevant software dependencies.
- Maintained monitoring for signs of potential exploitation and prepared remediation measures where required.

Signify Commitment

Protecting our customers, products, and services remains a priority. Signify will continue to assess new information and take appropriate action to maintain the security and availability of its products and services. We follow secure processes as described in Professional Systems and Services | Signify Company Website.

Additional Information

This advisory reflects the information available and the status of Signify's assessment as of 22 October 2026. It may be updated if the ongoing validation identifies information relevant to customers.

Terms of Use

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