OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. ***Most importantly - If your organization require direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal- our team will work with you to ensure all necessary support is available through the member submission and RFI process.***

Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

PHP2Shell: Industrial Vendor Exposure and Additional PHP Security Advisory

Critical PHP vulnerabilities affect selected industrial products; a separate, configuration-dependent PHP issue has also been disclosed.

TLP:CLEAR	Publicly sourced briefing suitable for external distribution.

Data current as of: 26 October 2026 | **Audience:** Critical infrastructure operators, partners and prospective OT-ISAC members

Key judgment. PHP2Shell has confirmed exposure in selected industrial and OT-supporting products. The immediate concern is vulnerable, reachable web-facing services and management interfaces–not evidence of compromised industrial control processes.

Executive Summary

On 21 October 2026, PHP released fixes for two critical remote code execution (RCE) vulnerabilities–**CVE-2026-109618 and CVE-2026-109619**–collectively known as PHP2Shell. Both have CVSS v4.0 scores of 9.2. The Cyber Security Agency of Singapore (CSA) reports widespread exploitation attempts and urges immediate remediation of internet-facing PHP deployments. [1–2]

Industrial product exposure is now documented. Security bulletins published between 22 and 23 October identify affected software and appliances used in process control, manufacturing execution, industrial edge environments, building management and network administration. These are product-level disclosures, not reports of OT intrusion. [3–7]

Confirmed Industrial Vendor Advisories

Selected public advisories as of 26 October 2026. Product versions and remediation status must be verified with each vendor.

Vendor	Named products / components	Advisory
Schneider Electric	EcoStruxure Security Expert (before 1.48.4.0); ProLeiT LINEoptimize; EcoStruxure Control Engineering	SESB-2026-295-01 [3]
ABB / B&R	APROL; selected ABB MES DokuWiki installations	SA26P015; 4HZK000017 [4]
Siemens	RUGGEDCOM APE1808 running specified PAN-OS releases	SSA-566512 [5]
Delta Controls	enteliWEB and selected V4 building-control products; scope and patch status vary	SecB0015 [6]
Belden	macmon and NetModule NRSW	PSIRT-10 [7]

Vendor notices above relate to the original PHP2Shell CVEs (CVE-2026-109618 / -109619), not the additional issue disclosed on 23 October.

Separate PHP Vulnerability: CVE-2026-115560

On 23 October, PHP also disclosed CVE-2026-115560, a separate and currently unpatched potential RCE vector that depends on an unusual combination of session serializer settings, a runtime switch to the php handler, and enabled session upload progress. PHP considers the circumstances unlikely and plans to address the issue in its regular release cycle. [1]

Interim guidance: set **session.upload_progress.enabled=0** at the applicable server or PHP worker configuration level after checking application dependencies. Organisations that already applied and validated this mitigation for PHP2Shell need not repeat it for the new CVE. The October 21 PHP releases do not patch CVE-2026-115560. [1]

OT/ICS Implications

Affected industrial software or web-management services may be situated within OT-supporting zones or provide access to maintenance and administrative functions. Where those components are reachable by an attacker, exploitation could enable compromise of a supporting host or service and create a pathway toward operational disruption. The consequence depends on deployment architecture, segmentation, privileges and recovery dependencies; an affected-product listing is not proof of exploitable network access or OT compromise.

Recommended Actions

- **Inventory and verify.** Identify PHP installations and vendor-supplied products, including embedded components; confirm versions against official bulletins.

- **Patch with priority.** Apply vendor-approved PHP2Shell fixes first to internet-facing and operationally critical deployments. Test OT changes through established maintenance processes.
- **Restrict access.** Reduce exposure of management interfaces, remote-access portals and supporting web services to trusted administration paths.
- **Validate the new mitigation.** Review session handler behaviour and verify session upload progress is disabled in the actual web-serving PHP configuration, not only in command-line PHP.
- **Investigate suspicious activity.** Examine web, system and endpoint logs for exploit attempts, unexpected process execution and anomalous access; preserve evidence before disruptive remediation.

OT-ISAC Assessment

OT-ISAC assesses that industrial vendor disclosures elevate PHP2Shell from a general web-application concern to a verifiable OT-supporting technology exposure. Operators should prioritise affected products according to accessibility and operational criticality, not severity scores alone. Public reporting reviewed as of 26 October does not establish that these vulnerabilities have compromised industrial control processes.

Assessment confidence: High for vendor-disclosed product scope; Moderate for deployment-dependent operational implications.

Reference Sources

[1] PHP Security Team – 21 and 23 October advisories
[2] CSA Singapore – Critical Vulnerabilities in PHP (PHP2Shell)
[3] Schneider Electric – Security Notifications (SESB-2026-295-01)
[4] ABB – Cyber Security Alerts (SA26P015; 4HZK000017)
[5] Siemens ProductCERT – SSA-566512
[6] Delta Controls – SecB0015
[7] Belden – PSIRT-10