Omron Robotics Security Advisory

PHP Vulnerabilities (PHP2Shell) – CVE-2026-109618 and CVE-2026-109619

Field	Value
Advisory ID	ORS-SA-2026-001
Publication date	30 October 2026
Last update	30 October 2026
Version	1.0
Classification	Public / TLP:CLEAR
Severity	Critical – CVSS v4.0 9.2 (PHP security team rating)
Status	Under investigation – this advisory will be updated as information becomes available

1. Overview

Omron Robotics is aware of the critical vulnerabilities recently disclosed in PHP, a widely used open-source server-side scripting language, tracked as CVE-2026-109618 and CVE-2026-109619 and collectively referred to as "PHP2Shell". Successful exploitation could allow an unauthenticated remote attacker to execute arbitrary code on systems running affected PHP versions.

Our Product Security Incident Response Team (PSIRT) is actively assessing the impact on Omron Robotics products, including any embedded web servers, configuration interfaces and software components that may bundle PHP. This advisory will be updated regularly until the investigation is complete.

In the meantime, customers should immediately ensure that the cybersecurity best practices and mitigations described in this advisory are applied across their operations.

2. Vulnerability Details

On 21 October 2026, the PHP project released security updates addressing two critical vulnerabilities in the PHP runtime. Every PHP installation that serves web requests is potentially at risk, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. A demonstrated exploit shows that a single unauthenticated request can trigger the attack before any application code runs. Public proofs of concept have begun to circulate.

CVE ID	CVSS v4.0	Description
CVE-2026-109618 GHSA-w8hw-w9fx-j79w	9.2 Critical	Memory corruption during out-of-memory (OOM) handling. When a request exceeds memory_limit, PHP can be interrupted while internal request data (e.g., a multipart file upload) is only partially initialised. Request cleanup may then free memory that was never initialised and which may contain attacker-controlled data, leading to remote code execution.
CVE-2026-109619 GHSA-6wmf-4rv5-p3rp	9.2 Critical	Use of stale global state. Request-owned internal state can survive after its backing memory has been freed (e.g., after a fatal error). A later request handled by the same worker may use that stale state before normal initialisation resets it, leading to remote code execution.

Affected PHP versions

- PHP 8.5 prior to 8.5.12
- PHP 8.4 prior to 8.4.27
- PHP 8.3 prior to 8.3.36
- PHP 8.2 prior to 8.2.35
- End-of-life branches (PHP 8.1 and older), which no longer receive updates from the PHP project

Note: On 23 October 2026, PHP disclosed a further RCE vulnerability, CVE-2026-115560, affecting only unusually configured web applications. It is not covered by this advisory; Omron Robotics is monitoring it and will address it in a future update if relevant.

3. Affected Products, Remediations and Mitigations

As of the date of this publication, Omron Robotics is assessing the following products. The status of each product will be updated to Affected, Not Affected or Fixed as the investigation progresses.*

Product	Versions	CVEs	Status	Remediation / Mitigation
SetNetGo (SNG)	SNG 7.x - PHP 5.6.24-0 SNG 8.x - PHP 8.1.22 SNG 9.x - PHP 8.2.34	CVE-2026-109618 CVE-2026-109619	**Affected**	A patch will be provided for SNG 8.x and 9.x. Apply the Recommended Mitigations below until the patch is installed. SNG 7.x requires the Recommended Mitigations below or an upgrade to a supported version of FLOW with a patched version of SNG 8.x or 9.x when available.
Fleet Operations Workspace (FLOW) Core / Fleet Manager	All versions (TBC)	CVE-2026-109618 CVE-2026-109619	**Affected**	Assessment in progress. Apply the Recommended Mitigations below until product-specific information is published.
Autonomous Mobile Robots – LD series (LD-60/90/250), HD-1500, MD series (onboard software)	All versions (TBC)	CVE-2026-109618 CVE-2026-109619	**Affected**	Assessment in progress. Apply the Recommended Mitigations below until product-specific information is published.

**As of the date of this advisory.*

Known not affected products

Product	Reason
MobilePlanner	PHP is not present in this product (Component Not Present)
TM Collaborative Robots (TM S / TM series) – TMflow	PHP is not present in this product (Component Not Present)
SmartController EX / eMotionBlox (eMB) robot controllers (i4, eCobra, Viper, Quattro)	PHP is not present in this product (Component Not Present)
Automation Control Environment (ACE)	PHP is not present in this product (Component Not Present)

4. Recommended Mitigations

Only updating PHP fully remediates these vulnerabilities. Until Omron Robotics publishes product-specific fixes, customers should apply the following measures to reduce the risk of exploitation:

1. Ensure robot controllers, mobile robots, fleet management servers and engineering workstations are not accessible from the Internet.
2. Isolate robot and control system networks from the business network using firewalls, and restrict access to web and configuration interfaces to authorized hosts only.
3. Where remote access is required, use secure methods such as Virtual Private Networks (VPNs), kept updated to the most current version.
4. Monitor web and configuration interfaces for unexpected requests, crashes or worker restarts, which may indicate exploitation attempts.
5. For customer-managed servers hosting Omron Robotics software alongside PHP (e.g., third-party web applications), update PHP to 8.5.12, 8.4.27, 8.3.36 or 8.2.35 or obtain patched distribution packages from your operating system vendor.

5. General Security Recommendations

Omron Robotics strongly recommends the following industry cybersecurity best practices:

- Locate control and robot system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so that no unauthorized personnel can access robots, controllers, peripheral equipment and networks.
- Never connect programming or engineering software to any network other than the network intended for that device.
- Scan all removable media (USB drives, etc.) before use in terminals or any node connected to these networks.
- Minimize network exposure for all control system devices and ensure they are not accessible from the Internet.
- Apply a defense-in-depth approach aligned with IEC 62443 and keep an up-to-date asset inventory, including third-party software components (SBOM).

6. References

- PHP security announcement: https://www.php.net/archive/2026.php#2026-10-21-5
- GHSA-w8hw-w9fx-j79w (CVE-2026-109618): https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
- GHSA-6wmf-4rv5-p3rp (CVE-2026-109619): https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
- CERT-EU Security Advisory 2026-018 – Critical Vulnerabilities in PHP
- NCSC UK – Critical security issue affecting PHP
- NCSC-NL inventory of products with PHP dependency: https://github.com/NCSC-NL/php2shell

7. For More Information

This document provides an overview of the identified vulnerabilities and the actions required to help mitigate them and is issued in accordance with the Omron vulnerability handling policy. To report vulnerabilities or request further information, contact Omron PSIRT:

- **PSIRT contact:** **OMRON Product Security Incident Response Team (PSIRT)**
- **Local support:** contact your Omron Robotics sales or service representative.

8. Legal Disclaimer

THIS ADVISORY AND THE INFORMATION CONTAINED HEREIN ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OMRON MAKES NO WARRANTY THAT THIS ADVISORY WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL OMRON BE LIABLE FOR ANY DAMAGES ARISING FROM THE USE OF THIS ADVISORY. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. OMRON RESERVES THE RIGHT TO UPDATE OR CHANGE THIS ADVISORY AT ANY TIME.

9. Revision History

Version	Date	Description
1.0	30 October 2026	Initial release. Products under investigation: SetNetGo (SNG), FLOW Core / Fleet Manager, AMR (LD, HD, MD series)