STERIS Cybersecurity Advisory

Third Party Vulnerability: PHP							
Initial Date	2026-10-30	**Date Revised**	N/A	**Doc. Version**	1	**Doc. #**	SAN-2026-00001

This cybersecurity advisory provides information regarding CVE-2026-109618 and CVE-2026-109619, two vulnerabilities in certain third-party PHP software components that have been publicly identified as critical, and describes STERIS's assessment and remediation activities.

STERIS is providing this update to inform Customers on which STERIS products were identified as using the affected PHP software components and to communicate the results of STERIS's assessment and remediation activities related to these third-party vulnerabilities.

As of the date of this advisory, STERIS is not aware of any exploitation of these vulnerabilities affecting STERIS products and has not received any reports of such exploitation on any STERIS products.

VULNERABILITY DETAILS

The vulnerabilities may enable remote code execution (RCE) when exploited under specific conditions. Links to additional information about these vulnerabilities are provided at the end of this advisory.

These vulnerabilities affect PHP, a widely used third-party software component, and are not specific to STERIS products.

STERIS PRODUCTS IDENTIFIED AS USING AFFECTED PHP VERSIONS

Based on STERIS's assessment to date, the following STERIS product was identified as using the affected versions of PHP:

- **ConnectCare℠ Technology Platform**

NOTE: This list may change based on updated information resulting from ongoing evaluations of additional STERIS products. If additional affected products are identified, STERIS will update this advisory accordingly.

REMEDIATION

No action is required by STERIS Customers.

STERIS completed deployment of a patch addressing CVE-2026-109618 and CVE-2026-109619 for the ConnectCare℠ Technology Platform on October 23, 2026. Based on STERIS's assessment, the ConnectCare℠ Technology Platform is no longer affected by these vulnerabilities.

STERIS will continue to monitor developments related to these vulnerabilities and will update this advisory if additional information materially changes our assessment or remediation guidance.

FOR MORE INFORMATION

For product or site-specific concerns, contact connectcare_support@steris.com. Please reference this advisory number SAN-2026-00001 when making inquiries. For more information regarding these vulnerabilities, please refer to the following resources:

- NVD-CVE-2026-109618
- NVD-CVE-2026-109619
- Critical Vulnerabilities in PHP Require Immediate Patching | CISA
- PHP: News Archive - 2026

This advisory is provided for informational purposes only and reflects information available to STERIS as of its date. It does not modify, expand, or create any warranty, representation, or obligation under any agreement between STERIS and its Customers. Third-party information referenced in this advisory is provided by its respective sources, and STERIS is not responsible for its accuracy or completeness.

We appreciate your cooperation. As always, STERIS is dedicated to supporting our products and valued Customers.