

Critical PHP Security Vulnerabilities

What these vulnerabilities mean for your website and what to do next.

Date: October 22, 2026 | **Severity:** Critical

Dear TSTS Customer,

We want to make you aware of two recently disclosed **critical security vulnerabilities affecting PHP**, a technology used by many websites and web applications. Public proof-of-concept information is circulating, making prompt review and remediation important.

9.2

CVSS v4.0 score

Critical

Severity rating

2

CVEs disclosed

IMPORTANT

The vulnerabilities are identified as **CVE-2026-109618** and **CVE-2026-109619** and are rated **Critical** with a CVSS v4.0 score of 9.2. They could allow **remote code execution** in affected PHP environments.

What this means for you

If TSTS Hosts and Maintains Your Website

TSTS has already addressed this for you.

Our team actively reviewed the websites and environments under our care and coordinated the necessary security updates and remediation. Provider-hosted websites were largely patched, with follow-up verification and remediation continuing where needed.

If TSTS Does Not Maintain Your Website

Please do not assume your website or other PHP-based systems have been updated.

Contact your website hosting provider, web developer, or IT provider and ask them to confirm that every PHP version used by your systems has received the applicable security update.

- Verify that all active PHP versions have received a vendor-supported patch or approved backport.
- Confirm that PHP-FPM or the applicable web service was restarted after the update.
- Ask specifically whether CVE-2026-109618 and CVE-2026-109619 have been addressed.

Need help determining whether you are protected?

TSTS can help **review your environment**, identify what actions may be needed, and **remediate**.

Protecting our customers is a priority, and our team has been actively responding across the environments we support.

Thank you for your continued trust in Twin State Technical Services.