

PHP2SHELL

CRITICAL PHP REMOTE CODE EXECUTION VULNERABILITIES

CVE-2026-109618 | CVE-2026-109619

CRITICAL

CVSS v4.0 9.2

Unauthenticated RCE risk in affected PHP web runtimes



ACTION REQUIRED: Inventory • Patch • Restart • Hunt • Validate

Advisory ID: PRIME-SOC-2026-10-023

Issued: 23 October 2026 | Classification: Customer advisory

www.primeinfoserv.com

01 / EXECUTIVE SECURITY BRIEF

Why this matters

An infrastructure-level weakness can bypass otherwise secure application controls.

Two critical PHP runtime vulnerabilities, collectively called PHP2Shell, can permit unauthenticated remote code execution (RCE) under exploitable conditions. The PHP project issued fixed versions on 21 October 2026 and urged immediate updating.

Because these defects affect PHP request processing, application authentication, plugin updates or an application-level WAPT exercise alone do not remediate a vulnerable runtime. Exploitability depends on the deployed version and execution environment.

WHAT IS EXPOSED?

Websites, APIs, customer portals, e-commerce, CMS platforms and third-party applications that serve web traffic using affected PHP runtimes.

BUSINESS CONSEQUENCES

Potential theft of secrets, application compromise, service disruption, unauthorised changes and downstream access through compromised credentials.

PRIORITISE INTERNET-FACING DEPLOYMENTS

- Identify owners, business criticality and hosting model for all PHP services.
- Include PHP-FPM, Apache mod_php, php-cgi, FrankenPHP and LiteSpeed.
- Treat outdated and unsupported PHP branches as urgent remediation items.

SOC POSITION

Patch first. Then investigate exposure-period activity; absence of alerts is not proof that exploitation did not occur.

02 / VULNERABILITY DETAILS

How exploitation can unfold

A crafted web request can trigger vulnerable memory-handling conditions.

TWO TRACKED VULNERABILITIES

CVE-2026-109618

Out-of-memory error handling can leave invalid request state and lead to memory corruption with possible code execution.

CVE-2026-109619

Stale request-specific state can be referenced after its backing memory is freed, enabling use-after-free risk.

HOW PHP2SHELL EXPOSURE CAN UNFOLD

01 REQUEST

Crafted HTTP request

02 RUNTIME

Vulnerable PHP memory handling

03 OUTCOME

Potential code execution

04 IMPACT

Data or server compromise

Potential outcomes depend on the environment; patching is the complete fix.

UNDERSTAND THE BOUNDARY

The attack may occur while PHP processes request data, before the application executes its own business logic. A vulnerable installation is not automatically compromised; successful exploitation depends on conditions and attacker capability.

Key consideration: patching the PHP runtime itself is essential; updating only WordPress, Laravel, plugins or other application packages is insufficient.

03 / REMEDIATION GUIDANCE

Patch now. Verify the active runtime.

Vendor security backports require package-level verification.

FIXED UPSTREAM PHP VERSIONS

PHP 8.2

FIXED: 8.2.35

PHP 8.3

FIXED: 8.3.36

PHP 8.4

FIXED: 8.4.27

PHP 8.5

FIXED: 8.5.12

REMEDIATION RUNBOOK

- **INVENTORY:** Include production, staging, containers, side-by-side installations, managed hosting and bundled software.
- **UPDATE:** Apply an official fixed PHP release or verified distribution/vendor security backport.
- **RESTART:** Restart PHP-FPM, Apache, LiteSpeed or affected container workloads to activate the patch.
- **VALIDATE:** Check both package status and the effective PHP versions serving requests. CLI `php -v` alone is not sufficient.
- **RETEST:** Confirm service availability and application behaviour; document owner, change record and evidence.

IMPORTANT

No complete workaround replaces updating. If patching cannot be completed promptly, reduce or remove exposure while following vendor and incident-response guidance.

04 / SOC THREAT HUNTING

What should your SOC investigate?

A targeted investigation complements patch deployment.

HIGH-VALUE TELEMETRY SOURCES

WEB & WAF

POST / multipart request anomalies, HTTP error spikes, request-size outliers, unusual patterns.

PROCESS & EDR

PHP or web-worker processes invoking shells, unexpected child processes, unapproved binaries.

FILE INTEGRITY

New or modified scripts in upload, temporary, cache or public directories; cron changes.

NETWORK & IDENTITY

Unexpected outbound traffic, unusual administrative accounts, unexplained secret access.

CLOUD & CONTAINERS

Runtime image provenance, recreated workloads, patch state, container process anomalies.

IF COMPROMISE IS SUSPECTED

Contain affected hosts, preserve logs and forensic evidence, review lateral movement, rotate exposed secrets, rebuild from known-good images where justified, and validate restoration before reconnecting.

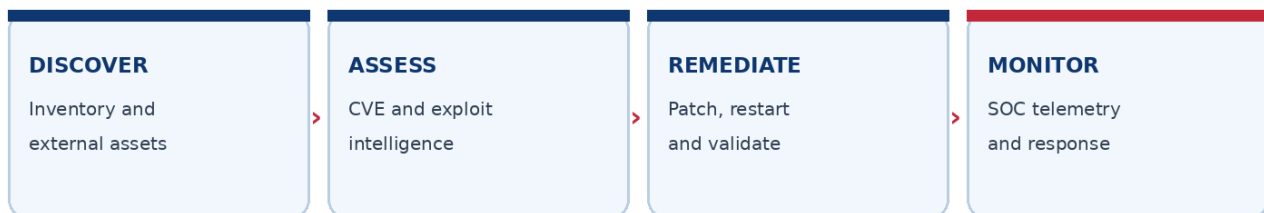
SOC rule: treat detection results as investigative indicators, not definitive evidence of compromise or safety.

05 / INTEGRATED DEFENCE

From patching to resilience

Coordinate asset discovery, vulnerability management and security operations.

BUILD A CONTINUOUS EXPOSURE-RESPONSE LOOP



Connect EASM, infrastructure VA, WAPT, threat intelligence and incident response.

RECOMMENDED ACCOUNTABILITY MATRIX

Infrastructure / Cloud

Confirm runtime inventory, patch, restart and validate.

App owners / DevSecOps

Perform regression tests; review runtime dependencies.

SOC / MDR

Retrospective hunt, monitor exploits and investigate anomalies.

Risk / Governance

Document decisions, status, exceptions and escalation.

PRIME INFOSERV | SECURITY OPERATIONS ADVISORY

Relevant capabilities: EASM, infrastructure vulnerability assessment, WAPT, threat intelligence, managed SOC and incident-response readiness.

06 / EXECUTIVE ACTION SHEET

Actions to close this advisory

Use this page as a customer-facing verification checklist.

01

Inventory all internet-facing and internal PHP runtimes

Asset owner and asset list recorded

02

Confirm affected versions and vendor backport status

Evidence linked to vulnerability record

03

Apply fixes and restart active workers

Change evidence and active runtime validated

04

Review logs and telemetry for the exposure window

SOC investigation and findings documented

05

Confirm any suspected intrusion is fully investigated

Containment, forensics and credentials reviewed

06

Retest applications and close verified findings

Risk owner signs off on closure

CUSTOMER NEXT STEP

Share this advisory with the infrastructure, application and SOC owners. Assign a closure owner and track verification evidence.

07 / SOURCES AND NOTICE

Reference notes

This is a defensive advisory; confirm applicability against vendor guidance.

VERIFIED TECHNICAL REFERENCES

PHP project security advisory and fixed releases

<https://www.php.net/>

Google Cloud response guidance

<https://cloud.google.com/blog/products/identity-security/responding-to-core-php-vulnerabilities-cve-2026-109618-cve-2026-109619>

Qualys technical analysis

<https://blog.qualys.com/vulnerabilities-threat-research/2026/10/20/php-announces-critical-security-release-for-two-vulnerabilities>

NHS England Digital cyber alert CC-4875

<https://digital.nhs.uk/cyber-alerts/2026/cc-4875>

Canadian Centre for Cyber Security alert AL26-026

<https://www.cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619>

ADVISORY STATUS

Information current as at 23 October 2026. Attack activity, advisories and vendor guidance may change. Verify version applicability and patched-package status against authoritative updates.

PRIME INFOSERV PVT. LTD.

Cybersecurity | Security Operations | Digital Resilience

www.primeinfoserv.com