TATA COMMUNICATIONS

PHP2Shell: When Vulnerabilities Move Faster Than Your Defences

An Executive Guide to vulnerability management and cyber resilience in the age of AI



Cyber Security Services by Tata Communications

TATA COMMUNICATIONS

Executive Summary

PHP2Shell is an urgent vulnerability. It is also a wider lesson in cyber readiness.

Two critical vulnerabilities in the PHP runtime, CVE-2026-109618 and CVE-2026-109619, can allow unauthenticated remote code execution under affected conditions.

The vulnerabilities affect core areas of PHP's operation, including memory management and error handling. Their position within the PHP runtime makes them relevant across applications and environments that depend on affected PHP versions.

For security teams, the immediate priorities are clear:

FIND : Identify affected PHP runtimes, particularly internet-facing and business-critical deployments.

PATCH : Upgrade affected systems to the applicable fixed PHP releases.

VERIFY : Confirm that updates have been applied correctly across servers, workers, containers and other affected environments.

INVESTIGATE : Determine whether exposed systems showed suspicious activity before remediation.

RESPOND : Contain and investigate systems where evidence warrants further action.

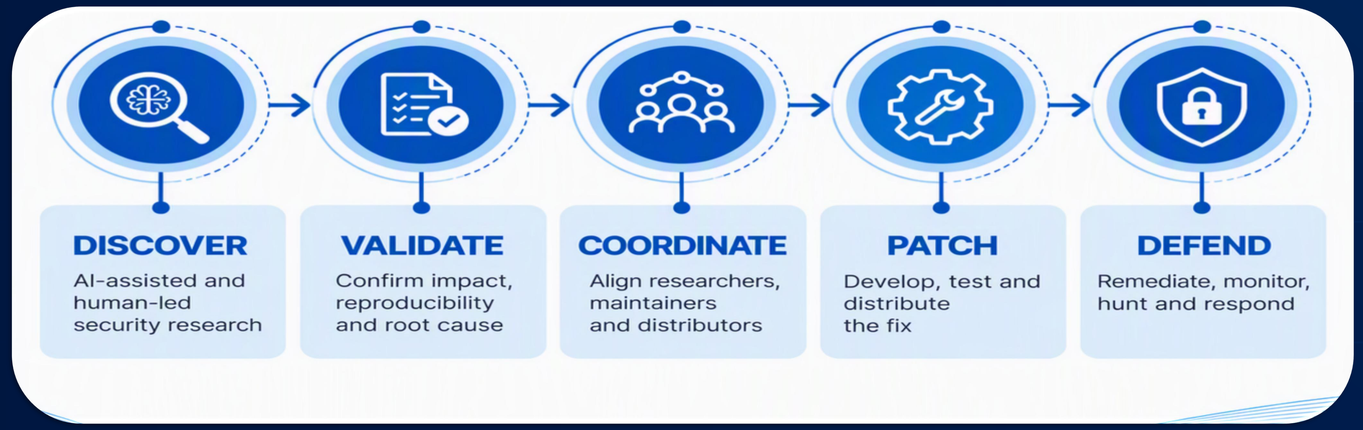
Patching closes the known vulnerability. It does not establish whether an exposed system was targeted before the patch was applied.



AI is changing the vulnerability timeline

The vulnerabilities emerged through a combination of traditional security auditing, independent research, AI-assisted discovery and human validation. The PHP Foundation's security programme has used tools including Anthropic's Claude Mythos and OpenAI's Daybreak Red alongside security audits, sanitizer builds and specialist research.

AI can help researchers find weaknesses, validate reports and connect findings that share the same root cause. But discovery is only the beginning. Human expertise remains essential to assess impact, make decisions, engineer fixes and coordinate disclosure.



What this means for enterprises

- Vulnerability discovery may accelerate
- Report volume and validation demands may increase
- Remediation must remain risk-led
- Detection must continue after patching
- Security operations need to stay connected

The Takeaway

Do we know every exposed instance of affected PHP, and can we prioritize remediation fast enough?

AI can accelerate discovery. Resilience depends on how quickly organizations turn that intelligence into protection.

5 Find. Patch. Verify

Know what is exposed. Prioritize what presents the greatest risk

CERT-In recommends identifying PHP usage, prioritizing internet-facing instances and upgrading affected deployments. CISA similarly calls for immediate patching to fixed PHP releases.

1. Find | Where is PHP running?
Identify affected PHP runtimes across servers, virtual machines, containers, hosting platforms and software products that bundle PHP.

2. Prioritize | What is exposed?
Give immediate attention to affected internet-facing systems, externally accessible applications and business-critical environments.

3. Patch | What needs to be upgraded?
Apply the applicable fixed PHP release: 8.5.12 | 8.4.27 | 8.3.36 | 8.2.35
Restart affected PHP workers and rebuild affected container images where required.

4. Reduce Exposure | What cannot be patched immediately?
Apply appropriate temporary safeguards while remediation is completed. Restrict unnecessary access, isolate unsupported systems and apply least privilege.

5. Verify | Did remediation remove the exposure?
Confirm the active runtime version, verify that workers and containers are updated, and identify systems that require further investigation.

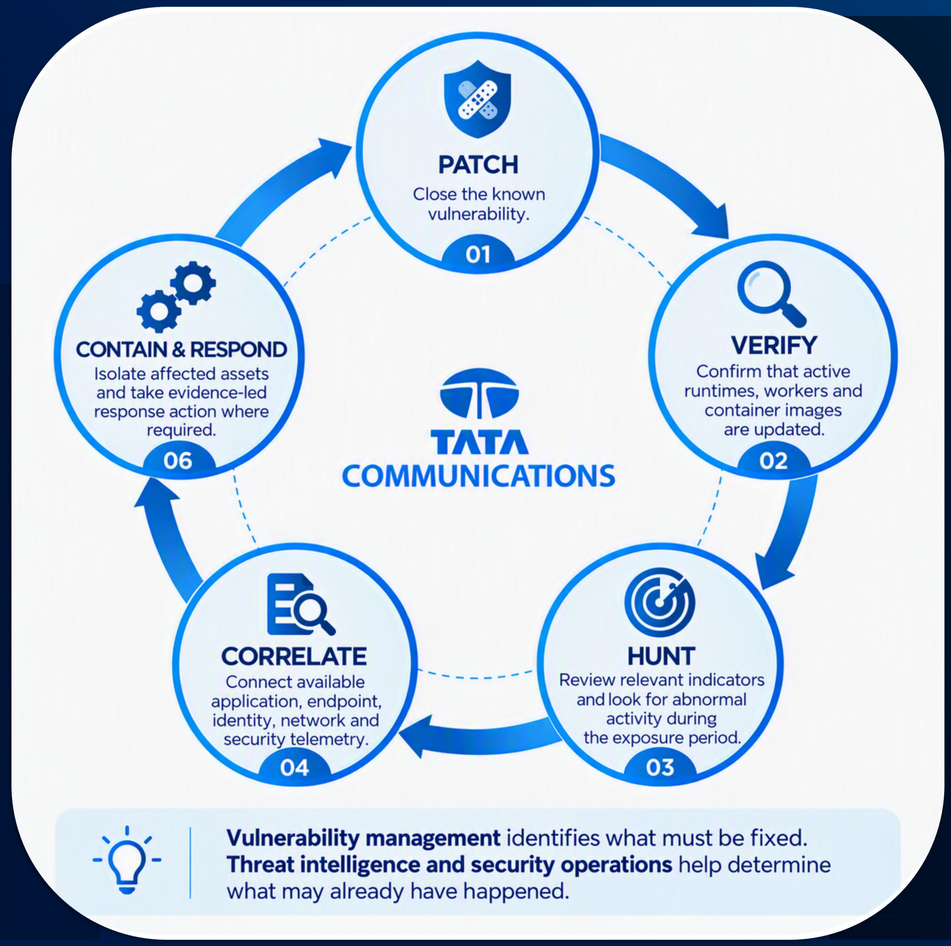
Remediation is complete only when the fix is applied, verified and connected to post-exposure investigation.

You patched PHP2Shell.

What happened before you patched it?

Applying the update closes the known vulnerability going forward.

It does not establish whether the system was targeted while it remained exposed. Security teams should connect remediation with retrospective investigation, relevant threat intelligence and available security telemetry.



Questions security teams should ask

- When was the affected system first exposed?
- What telemetry is available for the exposure period?
- Do relevant indicators appear in the environment?
- Is there evidence of suspicious process, network or identity activity?
- Does the system require containment or deeper forensic investigation?

TATA COMMUNICATIONS

How Tata Communications can help

Tata Communications helps enterprises connect vulnerability management, threat intelligence and security operations, supporting a faster journey from exposure identification to remediation, detection and response.

Our Cyber Security capabilities Include

Vulnerability Management and CTEM

Support vulnerability identification, exposure assessment, risk-based prioritization and remediation tracking across the attack surface

Cyber Threat Intelligence

Track evolving vulnerabilities, indicators and threat activity to support security awareness, detection and investigation



Managed Detection and Response / SOC Services

Provide continuous monitoring, investigation and response support through SOC-led security operations

Threat Hunting and Incident Response

Investigate potential compromise, correlate available evidence and support containment and incident response

Security advisory and Security Transformation Services

We work with enterprises to help

- Improve visibility into vulnerabilities and threats
- Prioritize action based on exposure and risk
- Connect remediation with monitoring and investigation
- Strengthen detection, response and operational resilience

TATA COMMUNICATIONS

The next critical vulnerability is not the question.
The question is how quickly your organization can find exposure, apply the fix and determine what may already have happened.

Find the exposure. |Fix the vulnerability. | Verify remediation. | Detect suspicious activity. | Respond effectively.

Strengthen Your Vulnerability and Detection Readiness

Engage with Tata Communications to connect vulnerability management, threat intelligence, detection and response.

tatacommunications.com

www.tatacommunications.com | @tata_comm

http://tatacommunications-newworld.com | www.youtube.com/tatacomms

©2025 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are registered trademarks of Tata Sons Private Limited.