



URGENT CLIENT ALERT

AI Exposes PHP Flaw— Immediate Action Required

Two critical vulnerabilities affecting PHP may allow a threat actor to remotely execute code on vulnerable systems. Security updates are available, and organizations should take immediate action.

Why This Matters

PHP is widely used in websites, web applications and other software. It can also be embedded in third-party products, meaning organizations may have exposure without realizing PHP is present in their environment.

Technical details and initial proof-of-concept code are circulating publicly, and security researchers have reported observing exploitation activity.

Treat this as an urgent patching event. Risk professionals should confirm that PHP exposure has been identified, internet-facing systems have been prioritized and available security updates have been deployed.

Key Questions for Risk Professionals to Ask

Risk professionals do not need to manage the technical remediation, but they should obtain clear confirmation that exposure is being identified, prioritized and addressed.

- Do we use PHP in our environment or within third-party applications?
- Have all internet-facing systems been identified and prioritized?
- Have the available security updates been deployed?
- Are we operating older or unsupported PHP versions?
- What is the remediation plan for systems that cannot immediately be updated?
- Are affected systems being monitored for suspicious activity?

Important: Installing the applicable security update is the only complete fix. Other measures may reduce exposure but do not eliminate the underlying vulnerabilities.

Cyber Insurance and Incident Response

Stay alert to any suspicious activity and if suspicious activity or evidence of compromise is identified, risk professionals should promptly involve the organization's information security, legal, incident response and cyber insurance teams.

Organizations should review applicable cyber insurance requirements involving:

- ✓ Incident or potential-claim notification
- ✓ Business interruption and data restoration
- ✓ Regulatory response
- ✓ Insurer-approved breach-response and forensic providers
- ✓ Privacy and network security liability

Bottom Line

This is not solely an IT issue.

Risk professionals should engage with your various teams, including marketing and web site developers and confirm that any PHP exposure has been identified, internet-facing systems have been prioritized, available security updates have been deployed, and systems that cannot immediately be remediated have a documented risk-reduction plan.

EPIC is not a law firm and does not provide legal advice. This communication is for general informational purposes only and is not intended to constitute legal advice or a recommended course of action. Consult counsel before making decisions or taking action concerning the matters discussed.



***Ready to be* EPIC?**

For more information about how EPIC can help your business, visit us at epicbrokers.com.