HSB

A Munich Re company

HSB ACTIVE THREAT MONITORING NOTIFICATION

Critical PHP vulnerabilities

HSB is committed to protecting policyholders from cyber risks and supporting recovery when incidents occur.

About HSB Cyber Safety

Policyholders who enroll in our Cyber Safety platform are proactively alerted about exposed credentials, exploitable vulnerabilities, and other issues that could impact them.

HSB will continue working with our threat intelligence partners to monitor the situation and will provide updates if there are any material changes.

- For general inquiries, email the HSB Cyber Concierge at cyber_concierge@hsb.com or schedule time to talk at http://concierge-scheduling.hsbcybersafety.com.
- To report a claim to HSB, email new_loss@hsb.co or call us at 888-HSB-LOSS (888-472-5677).
- To report a claim to HSB Canada, email claims@hsb.ca or call 1-888-988-0089.

Critical PHP vulnerabilities could allow attackers to take control of websites and servers

Two newly disclosed vulnerabilities in PHP, a programming language widely used to operate websites and web-based applications, may allow an attacker to run malicious commands on a vulnerable system without first logging in. In practical terms, successful exploitation could give an attacker control of an affected website or server. Because PHP is used within many common website platforms, custom applications, and hosting environments — including sites built on WordPress, Drupal, Joomla and other popular platforms — businesses may be exposed even if they are not aware that PHP is running behind their websites or online services.

Businesses should act promptly to determine whether PHP is used anywhere in their environment. This review should include public websites, customer and employee portals, e-commerce systems, hosted applications, and software managed by third-party technology or hosting providers.

There are steps that businesses can take to protect themselves.

- **Identify PHP systems.** Ask internal IT teams, website administrators, hosting providers, and managed service providers to identify every PHP installation, including PHP used within other applications. Prioritize systems that are accessible from the internet.
- **Install official security updates promptly.** Follow the PHP security advisory, and apply the appropriate PHP security release as soon as it is available and has been evaluated for your environment.
- **Address unsupported versions.** Upgrade PHP installations that are no longer supported.
- **Temporarily restrict access where necessary.** If a potentially vulnerable system cannot be patched immediately, consider limiting access through a virtual private network, approved IP addresses, or network isolation.
- **Contact third-party providers.** Businesses that use hosted websites, cloud applications, e-commerce services, or managed web platforms should ask their providers whether PHP is used, whether their systems are affected, and when security updates will be applied.
- **Do not rely solely on website scanning.** PHP may be embedded within applications or infrastructure that is difficult for external scanning services to identify.
- **Treat firewall protections as temporary safeguards.** Web application firewall rules may help reduce exposure, but they do not replace the official PHP security update.

What happened:

- Details of two critical PHP vulnerabilities, identified as CVE-2026-109618 and CVE-2026-109619, were disclosed online on October 20, 2026, before the planned security release.
- The vulnerabilities have been assigned a critical severity rating of 9.2 out of 10.
- A demonstration of an apparent exploit, referred to as "PHP2Shell," is circulating publicly, and unverified proof-of-concept exploit code has also been shared.
- At least one of the vulnerabilities has reportedly been reproduced by independent security researchers.

What we know:

- Early reporting indicates that PHP versions beginning with PHP 5 may be affected.
- The issue appears to affect PHP itself rather than one specific website platform.
- Successful exploitation could allow an attacker to take control of a vulnerable website or server, access sensitive information, install a persistent backdoor known as a web shell, or interrupt online services.
- Internet-facing systems present the most immediate concern because they can be reached directly by potential attackers.
- Shared hosting environments may face additional exposure because several websites can rely on the same underlying infrastructure.
- Reliable exploitation appears to require knowledge of the PHP version and other specific system conditions.

What we don't know:

- The actual number of vulnerable and exploitable systems is not yet known.
- Cloudflare has released emergency web application firewall rules intended to detect and block suspicious execution patterns, but protection against these specific vulnerabilities has not been confirmed.
- It is not yet clear how quickly attackers may develop reliable, automated exploitation methods.

HSB
One State Street
P.O. Box 5024
Hartford, CT 06102-5024
Tel: (800) 472-1866

hsb.com

© 2026 The Hartford Steam Boiler Inspection and Insurance Company. All rights reserved. This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms, or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form.
2026-196 (New 10/26)