



Critical PHP Vulnerabilities Advisory

October 27, 2026

Dear MIIA Member,

Yesterday morning, two critical vulnerabilities affecting PHP were disclosed: CVE-2026-109618 and CVE-2026-109619 (collectively dubbed “PHP2Shell”). Millions of web applications and websites rely on PHP, immediate action is required, as active exploitation is underway.

PHP is a popular server-side programming language used in the building of dynamic websites. WordPress is primarily powered by PHP, but WordPress sites are not the only potential targets, as other web applications, firewalls and critical perimeter security devices, can rely on PHP for their web-interfaces.

CVE-2026-109618 and CVE-2026-109619 affect all PHP versions, including unsupported versions. The vulnerabilities stem from improper error handling in the longjmp() function. If exploited, the vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code on a server.

Multiple proof-of-concepts (PoCs) have been released, and exploitation attempts are already being observed. Prior PHP vulnerabilities have been targeted by ransomware groups to compromise networks.

Mitigations and Recommended Action

Identify and inventory all PHP instances in your environment, all affected instances should be patched, if a patch cannot be applied, they should be removed from the internet.

If you are running PHP version 8.x, or unsupported versions 7.x and 5.x, it is critical that you update to the appropriate patched version, please follow vendor mitigation guidance:
<https://www.php.net/archive/2026.php#2026-10-21-5>

With Tokio Marine HCC – CPLG, we keep you at the forefront of emerging threats on the ever-evolving Cyber landscape. Our dedicated CTI (Cyber Threat Intelligence) team provides Active Domain Monitoring (ADM). The CTI team tracks current attack patterns and exposures by scanning customer networks, observing honeypot activity and malware logs, and monitoring sales and chatter in Dark Web markets. You also have access to our Cyber Incident Response team available 24/7/365 to answer questions and be your first line of defense when a ransomware incident occurs.

For all questions regarding your cyber insurance coverage, please contact your Account Executive and Risk Manager representatives.

Stay vigilant. Stay Cyber Strong®.

The MIIA Risk Management Team

@ 2026 MIIA. Solely for the benefit of MIIA members.
Disclaimer: The material contained herein is intended for general informational purposes only. It is not intended as legal advice and should not be construed as such. Any inquiries concerning Massachusetts law should be directed to a city solicitor, town counsel or other licensed attorney.

