October 22, 2026

Federal Agencies Warn of Critical PHP Security Vulnerabilities

Copyright Vermont League of Cities and Towns
Current as of: 11/16/2026



The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued an urgent warning regarding two newly identified vulnerabilities affecting PHP, a widely used programming language that powers websites and online applications.

According to federal officials, these vulnerabilities could allow threat actors to remotely execute malicious code on vulnerable servers without requiring valid credentials. Because PHP is extensively deployed across government, private-sector, and critical infrastructure environments, the potential impact could be significant.

What Organizations Should Do

Organizations that use PHP-based applications or web services should:

- Identify systems running affected PHP versions.
- Apply available security updates and patches immediately.
- Consider temporarily removing vulnerable systems from service if patches cannot be applied promptly.
- Monitor networks and systems for suspicious activity.

Copyright Vermont League of Cities and Towns
Current as of: 11/16/2026

- Follow internal incident reporting procedures and report confirmed compromises to appropriate authorities.

What This Means

Federal agencies emphasize that the warning does not indicate that PHP itself is inherently unsafe. Rather, these newly discovered vulnerabilities present a serious risk if left unpatched. The alert reflects the potential scale of exploitation and the importance of preventative action.

Potential Impacts

If exploited, these vulnerabilities could allow attackers to:

- Access sensitive information.
- Disrupt critical services and operations.
- Gain footholds for broader network compromise.

At this time, federal officials have not publicly confirmed a coordinated campaign by a foreign adversary exploiting these vulnerabilities. However, organizations are encouraged to act quickly to reduce risk and strengthen defenses.

Bottom Line

The strongest defense is timely patching. Organizations should review their PHP deployments immediately, apply available updates, and ensure vulnerable systems are properly secured.

Source: DHS Office of Intelligence and Analysis, based on NSA and CISA guidance.

Copyright Vermont League of Cities and Towns
Current as of: 11/16/2026