

TLP:CLEAR

October 21, 2026

Critical Vulnerabilities Discovered Impacting Popular Programming Language for Websites

Creators publish fixes for affected software

Please distribute the following information to your leadership, cybersecurity and information technology teams.

Two critical vulnerabilities have been discovered in Hypertext Preprocessor, or PHP, a widely-used open-source scripting language for web development, its creators announced today. This vulnerability reportedly impacts a vast majority of the world's websites. The vulnerabilities can allow unauthenticated remote code execution. The notice advises all PHP users to download updates immediately. The notice emphasizes that all PHP installations serving web requests are at risk.

Adding urgency to this vulnerability and to search for evidence of compromise is that [news of the vulnerability](#) was leaked on Oct. 19, two days prior to the patch being made available. Implementing the patches alone will not eradicate a hacker from your systems if the compromise occurred before patch deployment.

RECOMMENDATIONS

The [FBI](#) and [National Security Agency](#) recommend that organizations using PHP in their websites or web applications take the following steps immediately:

- Immediately implement the recommended [PHP updates](#).
- If an immediate update is not possible, take the system offline until an update can be made.
- Monitor web servers for suspicious activity, including unexpected command launches or file downloads.
- If you suspect a compromise, take action immediately and report to your local [FBI field office](#) or [www.ic3.gov](#).
- Maintain heightened cybersecurity vigilance and defensive measures.
- Maintain all records and evidence of suspicious cyber threat activity, as it will help local law enforcement, the FBI and other agencies assess the threat.

FURTHER QUESTIONS

For further questions or concerns, contact John Riggi, AHA national advisor for cybersecurity and risk, at jriggi@aha.org, or Scott Gee, AHA deputy national advisor for cybersecurity and risk, at sgee@aha.org. For the latest cyber and risk resources and threat intelligence, visit aha.org/cybersecurity.