



Risk | Insurance | Benefits | Retirement | Wealth

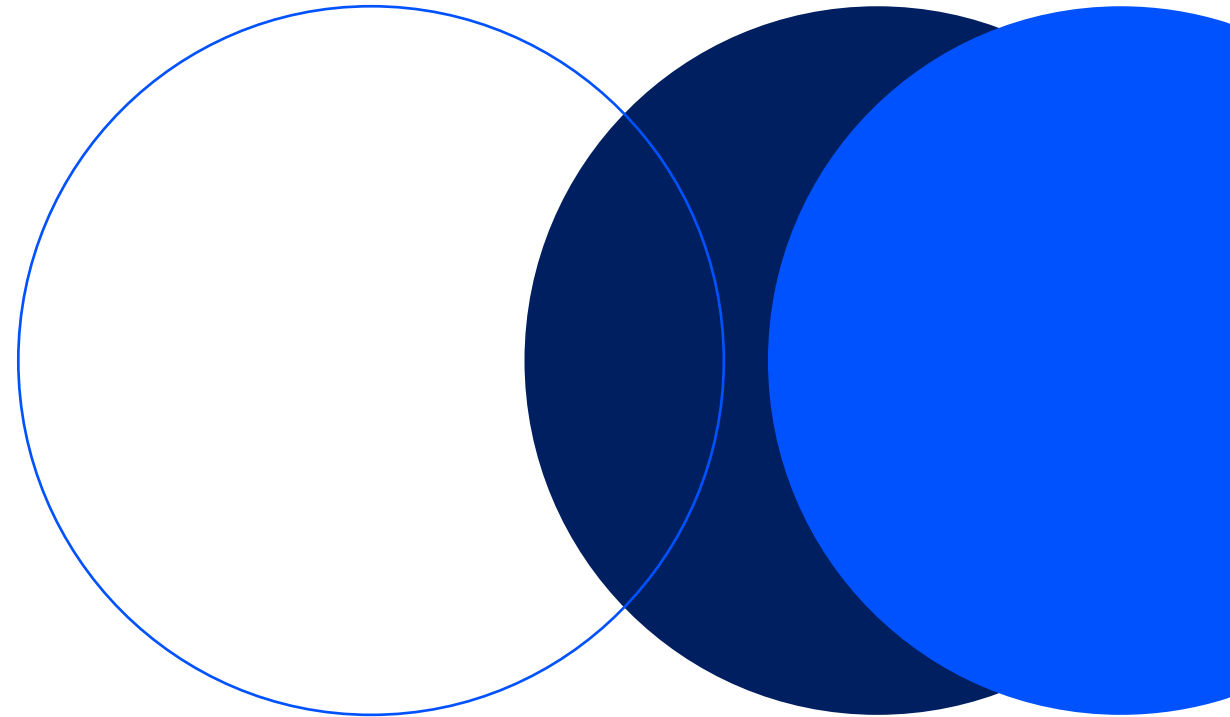
ProEx Cyber Alert

PHP Critical Warning



PHP WARNING

The PHP Foundation has issued a **WARNING** that programming language, released over 30 years ago and that powers a large share of websites and web applications, contains two critical vulnerabilities. There is potential that this vulnerability affects over 70% of the internet and more than 40% of websites. These exploits, if not fixed, could allow attackers to read sensitive data from server memory without taking over the server. Such data could include passwords, authentication tokens, API keys, and certificates. The PHP development team has released updates that “fix two critical vulnerabilities that can allow unauthenticated remote code execution. All PHP users are strongly encouraged to update immediately.” The FBI has advised, “If an immediate update is not feasible it is recommended that organizations take the system offline until it can be fully mitigated.”



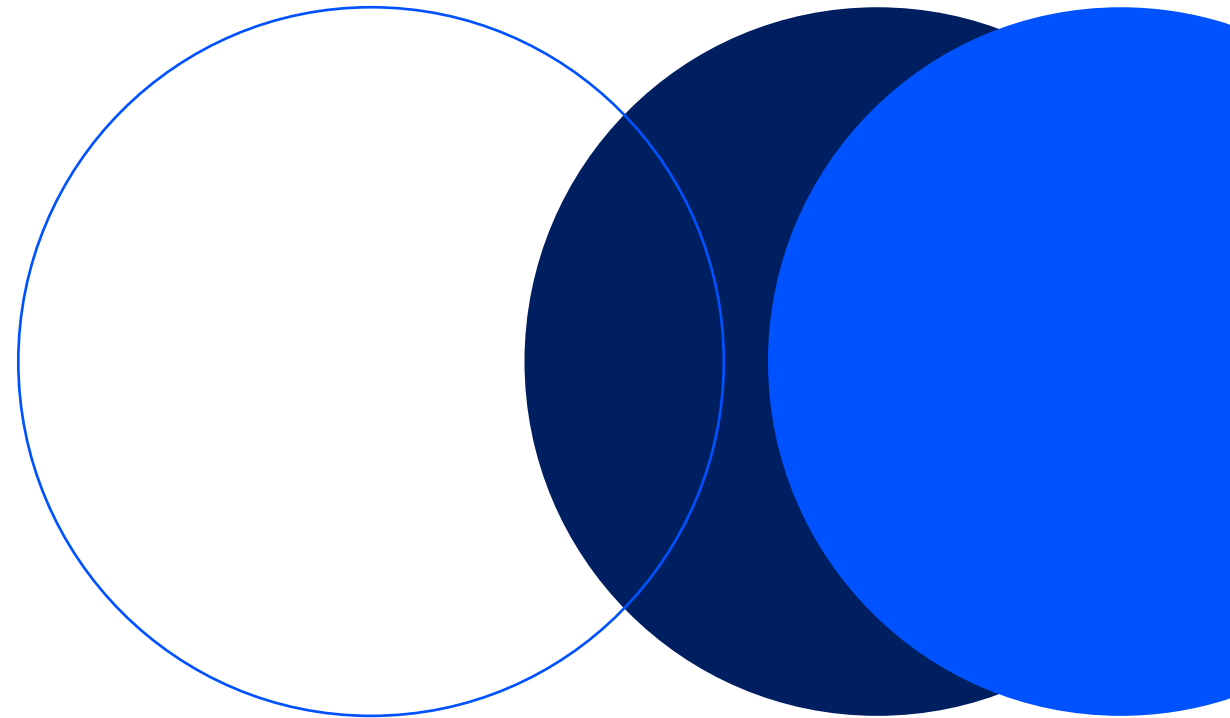
STEPS TO TAKE

-  **Identify Affected Systems**
Determine whether PHP is used across your organization, including internet-facing applications. Additionally, coordinate with third-party service providers to assess exposure and confirm whether the service providers have taken appropriate remediation measures.
-  **Immediately Patch**
Patching directions can be found on PHP's website directly: [PHP: News Archive - 2026](#)
-  **Mitigate Exposure**
If you are unable to immediately patch affected systems, per the FBI and PHP, you should take affected systems and applications offline until they are appropriately secured.
-  **Monitor For Potential Exploitation**
Monitor relevant logs for suspicious activity, including unexpected PHP processes launching shells, executing commands or downloading tools.

Does Cyber Insurance Respond?

While every Cyber policy is different, there may be coverage available if systems must be voluntarily shut-down or are exploited. There may be coverage if your organization experiences business interruption losses due to the shut-down or exploit. Remember that waiting periods and/or retentions may apply. If this is the case for your organization, you should notify your Cyber insurer immediately.

If you have any questions about your coverage or notification requirements, please contact your HUB broking team to consider providing notice to your Cyber carrier.



This alert does not consist of tax, business, or legal advice. Professional advice should be sought before taking action based on this information.

