

THIS WEEK'S AGENCY SECURITY BRIEF

A critical PHP flaw. A practical next step.

PHP and CISA issued urgent patch guidance on October 21, 2026.

Ask your website provider whether your agency's systems are affected and what fix is actually running.

OpenAI reports that AI-assisted research helped uncover a PHP flaw. Applying and verifying the fix still takes action.

FOUR QUESTIONS FOR YOUR WEBSITE PROVIDER

Who owns the fix?

- 1 Do any systems you run for us use PHP?
- 2 Have you addressed both PHP2Shell CVEs?
- 3 What evidence shows the fix is running?
- 4 Who owns anything still unresolved?

Get the provider's answer and keep the evidence. A working website does not prove the underlying software is patched.

AI AND YOUR AGENCY'S DEFENSES

Faster analysis. Verified action.

AI can help review approved code and configuration evidence, interpret advisories and organize priorities.

Keep the responsible person, the authorization and the verification attached to the work.

In its October 21 alert, CISA said it had not observed exploitation at publication. This brief is not a finding that your agency has been compromised.

BEFORE CONNECTING AI TO AGENCY INFORMATION

Check the permissions.

READ Which mailboxes, files and records?

SEND Draft only, or send and attach?

CHANGE Which records and settings?

DISCLOSE Where can information leave?

Use fictional records for an initial test. Outside instructions should not give the assistant new authority.

AGENCY AI SECURITY SPRINT

Get the first agreed gap closed.

\$750 one time. One website, one email environment and up to two AI workflows.

Evidence-backed priorities, a written action pack, one agreed improvement and a reusable team/provider handoff.

OpenAI cybersecurity access, applied to authorized defensive work.

Start with a free, 30-minute conversation. Scope, access and timing agreed first. Agreed review, improvement and handoff before billing.

cirlet.com/security

Sources and dated limits: cirlet.com/security-php2shell