

CISA urges immediate patching of critical PHP flaws known as php2shell



CISA urges immediate patching of CVE-2026-109618 and CVE-2026-109619 in PHP, which allow unauthenticated remote code execution. No exploitation has been observed so far, but fixed versions are available.

- Two critical PHP vulnerabilities, CVE-2026-109618 and CVE-2026-109619, are collectively called php2shell.
- They allow unauthenticated remote code execution and affect all PHP installations serving web requests.
- Fixed versions are PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35.
- CISA had not observed exploitation at the time of publication.
- PHP 8.1 and older no longer receive updates, so affected systems should be taken off the internet.

CISA has issued a strong call for organizations to patch two critical vulnerabilities in PHP, CVE-2026-109618 and CVE-2026-109619, together referred to as "php2shell".

What is affected

The flaws allow an unauthenticated attacker to execute code remotely, and they affect every PHP installation that serves web requests. The fixed releases are **PHP 8.5.12, 8.4.27, 8.3.36** and **8.2.35**. CISA notes that it had not seen exploitation when it published the alert, but unpatched systems remain at risk.

What CISA recommends

CISA advises organizations to first identify and inventory every system running any version of PHP. This matters because PHP is frequently embedded in other software, so its presence may not be obvious. Patches should then be applied as soon as they are available, with internet-facing systems first.

Where immediate updating is not possible, or where systems run PHP 8.1 or older, which no longer receive updates, CISA recommends taking those systems off the internet until they can be patched or upgraded. A web application firewall may offer some interim protection, but it is not a substitute for updating.

Why it matters for regulated institutions

Because exposure can sit inside third-party products, inventory is the step most likely to be incomplete. Institutions should ask vendors whether their products bundle PHP, and track remediation through the normal vulnerability and change management process.

What to do now

1. Inventory all systems and third-party products that run or bundle PHP, including those where it is not directly visible.
2. Update to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, starting with internet-facing systems.
3. Take systems that cannot be patched promptly, or that run PHP 8.1 or older, off the internet until they are updated.
4. Use a web application firewall as a temporary measure only, not as a replacement for patching.
5. Ask vendors to confirm whether their products include PHP and when fixes will be delivered.