

EXPLAINED IN 6 SLIDES

What is PHP2Shell and why should you care?

Two flaws in the PHP engine were disclosed on Wednesday, October 21, and by that same night millions of attack attempts were already being counted.

Two flaws in the PHP engine itself, rated 9.2 out of 10

CVE-2026-109618 and CVE-2026-109619 let anyone run code on servers with no username or password. They affect almost every version since 5.4, and Wiz showed attacks on WordPress, Drupal and Joomla.

Finding them with AI took a week; exploiting them, minutes after disclosure

Calif found the first on August 1 with an OpenAI model; Wiz got there alone on the 19th with AI agents. Cloudflare counted millions of attempts on patch night.

Update today or take the site offline, say PHP and CISA

PHP shipped fixed versions. CISA asked to disconnect whatever cannot be updated, especially PHP 8.1 or unsupported versions. The Netherlands and Finland took government sites offline as a precaution.

What changes for companies and public institutions in the region

In Costa Rica, MICITT alerted directors, IT heads and cybersecurity liaisons across the public sector. If your site runs PHP, someone decides today between patching and going offline.

The gap is more about governance and speed than technology

The patch is out. Many institutions still lack a CSIRT with a mandate, an inventory and someone with written authority to take a site offline. Who signs that at yours?