

EXPLICADO EN 6 LÁMINAS

¿Qué es PHP2Shell y por qué te toca?

Dos fallas en el motor de PHP se publicaron el miércoles 21 de octubre y esa misma noche ya se contaban millones de intentos de ataque.

Dos fallas en el motor de PHP con severidad 9,2 sobre 10

CVE-2026-109618 y CVE-2026-109619 permiten ejecutar código en un servidor sin usuario ni contraseña. Afectan casi todas las versiones desde 5.4, y Wiz demostró ataques contra WordPress, Drupal y Joomla.

Encontrarlas con IA tomó una semana; explotarlas, minutos tras el anuncio

Calif halló la primera el 1 de agosto con IA de OpenAI y Wiz llegó sola el 19 con sus agentes. Cloudflare contó millones de intentos la noche del parche.

Actualizar hoy o desconectar el sitio, dicen PHP y CISA

PHP publicó versiones corregidas. CISA pidió desconectar lo que no se pueda actualizar, en especial PHP 8.1 o versiones sin soporte. Países Bajos y Finlandia apagaron sitios públicos por precaución.

Lo que cambia para empresas e instituciones de la región

En Costa Rica, el MICITT alertó a directores, jefes de TI y enlaces de ciberseguridad del sector público. Si tu sitio corre PHP, alguien decide hoy entre parchar o apagar.

La brecha tiene más de gobernanza y velocidad que de tecnología

El parche existe desde el miércoles. Falta un CSIRT con mandato, un inventario y alguien con autoridad escrita para apagar un sitio público. ¿Quién firma eso en tu institución?