Tecnología

El día que internet tembló

El miércoles 21 de octubre coincidieron cinco incidentes de seguridad de alcance global, varios con la máxima gravedad posible. Seguimos las alertas desde la noche anterior, revisamos cada caso contra nuestra plataforma y ninguno comprometió los sistemas de Finnegans ni los datos de nuestros clientes. Acá contamos qué pasó, qué hicimos y por qué estamos tranquilos.

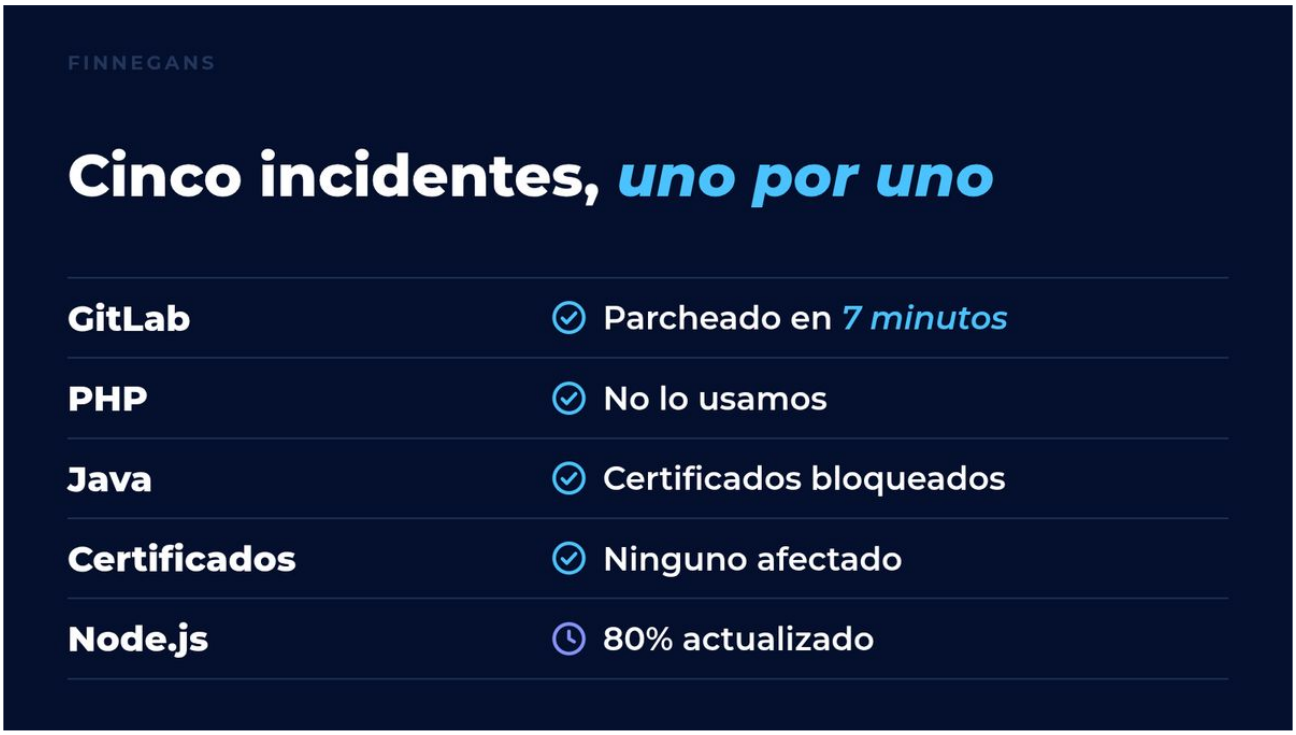
Por Mariano Casero · 22 de octubre de 2026

El alcance, en números

PHP2Shell fue, por lejos, el incidente de mayor alcance: tocó a la tecnología sobre la que funciona la mayoría de los sitios web del mundo.

En resumen

Los cinco incidentes tenían corrección disponible el mismo día: la clave era aplicarla antes que los atacantes.



PHP2Shell: la falla que puso en alerta a medio internet

PHP publicó el 21 de octubre parches de emergencia para dos fallas críticas en su motor (CVE-2026-109618 y CVE-2026-109619, severidad 9,2 sobre 10). Permiten que un atacante tome control de un servidor sin usuario ni contraseña.

El alcance es enorme: PHP está en cerca del 70% de los sitios web, incluidos todos los que usan WordPress, Drupal, Joomla, Magento o Laravel. Las fallas afectan a casi todas las versiones desde PHP 5.4 y se corrigen en 8.5.12, 8.4.27, 8.3.36 y 8.2.35. Las encontraron Wiz y Calif junto con OpenAI, con ayuda de inteligencia artificial.

La NSA recomendó actualizar de inmediato o desconectar los sistemas, y varios gobiernos europeos dieron de baja sitios de forma preventiva. Cloudflare reporta los primeros intentos de ataque.

En Finnegans: no nos afecta, y acá el momento jugó a favor. Hace aproximadamente un mes lanzamos el nuevo sitio de Finnegans, un desarrollo completamente nuevo que reemplazó al anterior, que sí estaba hecho en PHP. Hoy no usamos PHP en ningún sistema.

GitLab y Ruby: una falla de doce años

GitLab publicó una actualización crítica para CVE-2026-110264, con la máxima severidad posible: 10 sobre 10. Permite tomar control de un servidor GitLab propio sin credenciales, haciendo que el servidor muestre un archivo de texto preparado para eso.

El origen está en Onigmo, el motor de expresiones regulares que usa Ruby, el lenguaje en el que está construido GitLab. Afecta a todas las versiones desde la 7.0, de 2014. Se corrige en 19.5.1, 19.4.3, 19.3.6 y las versiones equivalentes de ramas anteriores. Ojo: las versiones parcheadas el 12 de octubre siguen siendo vulnerables.

GitLab.com ya estaba corregido; el riesgo es para quienes administran su propio servidor. No hay ataques reportados por ahora.

En Finnegans: esta sí nos tocaba. Nuestro equipo de seguridad aplicó el parche a los 7 minutos de publicada la corrección. Pudimos hacerlo así de rápido porque nuestra política de actualización de plataformas nos tenía en una versión muy cercana a la corregida. Revisamos los registros y no encontramos rastros de intentos de explotación. Ruby lo usamos solo dentro de GitLab, así que quedó cubierto con el mismo parche.

Node.js: diez vulnerabilidades en un mismo día

Node.js publicó versiones corregidas para sus tres líneas con soporte: 26.12.1, 24.22.1 y 22.23.4. Corrigen diez vulnerabilidades, cuatro de severidad alta.

La más seria es una falla en el descompresor Brotli que podría permitir ejecutar código de forma remota. Otras dos permitían saltear la verificación de los certificados de seguridad en ciertos casos, lo que abre la puerta a que un atacante se haga pasar por un servidor legítimo. La misma actualización deja de confiar en los certificados comprometidos de eMudhra. Las versiones de Node.js sin soporte siguen siendo vulnerables y no tienen parche.

En Finnegans: usamos Node.js en varios servicios. Al momento de publicar este post, el 80% ya está actualizado, incluidas todas nuestras imágenes de Docker. Los servicios que faltan están aislados y se actualizan en el transcurso del día.

Java y los certificados de eMudhra: cuando falla la confianza

Los certificados digitales son los que garantizan que, cuando un sistema se conecta a otro, está hablando con quien dice ser. Los emiten autoridades certificadoras, y los navegadores, sistemas operativos y lenguajes confían en ellas.

El 21 de octubre se supo que se comprometieron las claves privadas de ocho certificados intermedios de eMudhra, una autoridad certificadora de India. Esas claves podían calcularse en segundos, así que cualquiera podría emitir certificados falsos y hacerse pasar por un sitio legítimo. Mozilla, Google, Apple y Microsoft están retirando la confianza en esos certificados, y algunos expertos comparan el impacto con el de Heartbleed.

Java resultaba particularmente expuesto porque usa su propia lista de certificados de confianza y, por defecto, confiaba en ellos. Oracle emitió una alerta fuera de calendario (CVE-2026-91403, severidad 9,1) y OpenJDK publicó versiones corregidas (por ejemplo, 21.0.13.0.2 y 17.0.21.0.2). Node.js, en paralelo, empezó a bloquear esos certificados.

Ese mismo día, GoDaddy revocó por error algunos certificados SSL, lo que obligó a sus clientes a reemplazarlos.

En Finnegans: usamos certificados de eMudhra, pero ninguno coincide con las huellas digitales de los ocho comprometidos. Para cubrir el otro riesgo, el de confiar en un certificado falso al conectarnos con otros sistemas, bloqueamos a mano esos ocho certificados en Java. También verificamos que nuestros certificados de GoDaddy no estuvieran entre los revocados.

Finnegans 22 de octubre de 2026

Qué hicimos

La respuesta empezó antes de que el día arrancara y siguió a medida que cada aviso se hacía público.

Por qué no nos tomó desprevenidos

Un día como el 21 de octubre no se resuelve ese día: se resuelve con lo que se hace todos los otros.

- **Estamos certificados en ISO 27001.** Nuestros procesos de detección y corrección de vulnerabilidades están auditados, lo que los hace sistemáticos y eficientes.
- **Sabemos qué usamos.** Mantenemos un inventario de las tecnologías y versiones de cada sistema, así que ante un aviso sabemos en minutos si nos alcanza.
- **Actualizamos de forma continua.** Nuestra política de actualización de plataformas nos mantiene cerca de las últimas versiones. Por eso el parche de GitLab se aplicó en 7 minutos.
- **Monitoreamos de forma permanente.** Seguimos los avisos de seguridad de las tecnologías que usamos y revisamos los registros de nuestros sistemas.
- **Limitamos accesos y aislamos servicios.** Cada sistema tiene solo los permisos que necesita, y podemos aislar un servicio mientras lo actualizamos, como hicimos con Node.js.

- **Tenemos un proceso de respuesta.** Sabemos quién hace qué cuando aparece una alerta crítica.

Si gestionás tu propia infraestructura

Si en tu organización administran sistemas propios, estas son las revisiones que recomendamos hacer hoy:

- **PHP:** actualizar a 8.5.12, 8.4.27, 8.3.36 o 8.2.35. Incluye cualquier sitio en WordPress, Drupal, Joomla o Magento. Las versiones 8.1 y anteriores necesitan un parche de su proveedor o una migración.
- **GitLab propio:** actualizar a 19.5.1, 19.4.3, 19.3.6 o la versión corregida de su rama, aunque hayan parcheado el 12 de octubre.
- **Node.js:** actualizar a 26.12.1, 24.22.1 o 22.23.4.
- **Java:** actualizar a la versión corregida de su proveedor o bloquear los ocho certificados comprometidos de eMudhra.
- **Certificados:** actualizar los almacenes de certificados de confianza de servidores y equipos, y verificar que ningún certificado propio haya sido revocado.

Si sos cliente de Finnegans, no tenés que hacer nada respecto de nuestra plataforma: esa parte la gestionamos nosotros. Si tenés cualquier duda, escribinos por el canal de tecnología de nuestra comunidad de WhatsApp.

Fuentes

- TechCrunch — The internet is having a very bad cybersecurity day
- Wiz — PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet
- Patchstack — Major security alert: PHP vulnerable to critical RCE
- Rescana — GitLab CVE-2026-110264
- Cyber Kendra — Node.js October 2026 security releases
- Oracle — Security Alert CVE-2026-91403
- Lilting — Does Java trust eMudhra's compromised intermediate CAs?

Infografías

Finnegans

22 de octubre de 2026