Académico UV, Marco Aravena, analiza las vulnerabilidades en PHP y por qué los gobiernos bajan sus páginas de manera preventiva

Finlandia, Países Bajos y Francia sacaron de línea sitios de gobierno sin esperar a que existiera una solución. La razón son dos vulnerabilidades críticas en PHP, el lenguaje que está detrás de cerca de siete de cada diez sitios web. Al respecto, Marco Aravena, director general de Modernización y Transformación Digital UV señala que "la pregunta es cuánto nos afecta esto en Chile".

El académico de Ingeniería Civil Informática UV y candidato a doctor en Industria Inteligente explica que «una página web son archivos y programas guardados en un computador, también llamado servidor, que está siempre encendido y conectado a internet. Al escribir una dirección en el navegador, ese servidor prepara la página y la manda».

«PHP es el lenguaje con que muchos de esos servidores arman las páginas. Es lo que permite que un sitio deje de ser una página fija y pueda mostrar un carro de compras, validar una clave, cargar un curso en una plataforma educativa o publicar una noticia nueva. Según W3Techs, PHP lo usa cerca del setenta por ciento de los sitios cuyo lenguaje de servidor se conoce, es decir, casi siete de cada diez. PHP nació en 1994, creado por el programador Rasmus Lerdorf, y hoy lo desarrolla y mantiene una comunidad global conocida como The PHP Group», agrega.

Por qué el problema es tan masivo: los CMS

El académico añade que «casi nadie programa un sitio desde cero. Lo habitual es usar un CMS, sigla en inglés de sistema de gestión de contenidos. Un CMS es un programa ya armado que permite crear y administrar un sitio sin escribir cada página a mano: al subir un texto, una foto o un producto, el sistema se encarga del resto».

«Los CMS más conocidos están hechos en PHP: WordPress, Drupal, Joomla y Magento, este último muy usado en tiendas online. W3Techs mide que el cien por ciento de los sitios que usan WordPress funcionan sobre PHP, y WordPress está en alrededor del cuarenta por ciento de todos los sitios web», agrega.

«Por eso el alcance es tan grande. Si la falla estuviera en un plugin, que es una extensión que se le agrega al CMS para sumar funciones como un formulario de contacto o un carrito de compras, afectaría solo a quienes lo instalaron. Como está en PHP, que es el motor, el problema lo heredan todos los sitios construidos encima, aunque su CMS esté al día. En Chile hay sitios de gobierno, tiendas online y medios de comunicación levantados sobre estos sistemas», comenta.

Qué pasó: vulnerabilidad, ataque y PHP2Shell

Según explica el especialista «una vulnerabilidad es una falla en el código, como una cerradura mal diseñada. Que exista no significa que alguien haya entrado. Un ataque es cuando alguien aprovecha esa falla a propósito para entrar».

«Aquí son dos fallas críticas en PHP, con 9.2 sobre 10 en la escala CVSS que mide la gravedad. Permiten que una persona externa ejecute sus propios comandos en un servidor sin iniciar sesión, y eso puede terminar en robo de datos, un sitio alterado o el control completo del servidor. El caso circula con el nombre PHP2Shell», indica.

Aravena destaca que «fallas de ese tipo llevaban años presentes, pero se consideraban demasiado difíciles de aprovechar. Hay dos versiones de quién las encontró. Según el

WSJ, citado por BioBioChile, en agosto de este año el investigador Ryan Austin revisaba el código de PHP con ayuda de un modelo de inteligencia artificial de OpenAI y halló la manera de explotarlas. Según Reuters, citado por Las Últimas Noticias, el hallazgo fue de Wiz, empresa de ciberseguridad de Alphabet, con su herramienta Wiz Atlas y modelos de Google y OpenAI, y las fallas llevaban más de diez años ocultas en el código. Ambas coinciden en que la IA fue clave. El aviso a los responsables de PHP se dio el 11 de agosto y desde ahí se trabajó en la solución: cambios en unos doscientos archivos y más de diez mil líneas de código. Según Reuters, en la respuesta participaron Google Cloud, Cloudflare, AWS, Microsoft y Akamai. Un ingeniero de seguridad de la fundación de PHP lo calificó como el problema de seguridad más grave en más de diez años para este lenguaje y lo comparó con Heartbleed».

«La publicación del parche estaba prevista para este 22 de octubre, pero una filtración en Hacker News obligó a adelantarla. Cloudflare, una empresa intermediaria entre los visitantes y el servidor de un sitio para protegerlo y hacerlo más rápido, reportó intentos de ataque horas antes de que saliera, y por eso varios gobiernos prefirieron apagar sus sitios y esperar. En Países Bajos se desconectaron la propia agencia de ciberseguridad, el Puerto de Róterdam, el portal gubernamental Overheid.nl y varios hospitales. En Finlandia, el proveedor estatal Valtori sacó de línea los servicios de red pública del gobierno. En Dinamarca, Kombit suspendió la plataforma nacional de comunicación escolar, y en Francia el Ministerio del Interior puso todos sus sitios en mantenimiento preventivo. La reacción fue internacional: Estados Unidos evalúa el impacto en sus instituciones e infraestructura crítica y Japón emitió una alerta urgente, recomendando suspender temporalmente los servicios que no puedan actualizarse», agrega.

«Lo que más preocupa a los especialistas es lo que viene

después. Cuando se publica un parche, los atacantes lo comparan con el código anterior para descubrir qué se corrigió, y con inteligencia artificial ese trabajo se puede hacer mucho más rápido», asegura.

El parche y las versiones

El académico cuenta que «un parche es una actualización que corrige la falla, como cambiar la cerradura. PHP lo publicó el 21 de octubre en las versiones 8.5.12, 8.4.27, 8.3.36 y 8.2.35. Que un sitio use PHP no significa que esté hackeado. Significa que hay que confirmar que esté actualizado».

«Si un sitio corre en la 8.1 o anteriores, no hay versión oficial. Existen parches básicos de código fuente y algunas distribuciones de Linux preparan los suyos, así que es necesario consultar al proveedor. Hay que prestar atención también a la 8.2: el 31 de diciembre de 2026 llega al final de su vida y después de esa fecha no recibirá más parches de seguridad», señala.

Qué significa para Chile

En cuanto a la situación nacional, Aravena identifica que «en Chile hay páginas de gobierno, empresas, tiendas online, plataformas educativas y medios hechos con PHP y estos CMS. Si el servidor donde viven no se actualiza, quedan expuestos. El 21 de octubre el CSIRT Nacional de la ANCI publicó la alerta AVC26-00740, y la agencia pidió en sus redes que todas las organizaciones que usan PHP actualicen de inmediato. Que haya una alerta oficial no significa que haya sitios chilenos comprometidos. Significa que el riesgo es real y que el tiempo es corto».

Sobre cómo prepararse para prevenir estos ataques, el académico sugiere «consultar al proveedor de hosting para saber si actualizó PHP y a qué versión; en el caso de usar cPanel, entrar a Multi-PHP Manager para revisar qué versión usa cada dominio; si el proveedor administra el servidor,

pedir por escrito que instale el parche; respaldar antes de actualizar y comprobar que se pueda restaurar; si la versión de PHP ya no tiene soporte, realizar una migración porque el parche de emergencia no lo reemplaza; un firewall web, como el de Cloudflare, ayuda mientras tanto, pero es un paliativo y no sustituye la actualización».

Otra de las recomendaciones del experto es «si una institución está obligada por la Ley 21.663, es necesario revisar los canales del CSIRT Nacional y los plazos de reporte, junto con analizar las señales raras, como pueden ser cambios que no se realizaron, archivos desconocidos o redirecciones a otros sitios. Para quienes administran un sitio, hoy toca revisar. Por eso se sugiere contactar al proveedor, hacer un respaldo y confirmar la versión de PHP, lo cual toma poco tiempo comparado con recuperar un sitio comprometido».