Alerta Técnica
Vulnerabilidades críticas en PHP

LUMA

TLP:CLEAR

Prepare la actualización de sus servicios PHP y priorice los expuestos a Internet. El equipo de PHP anunció dos fallas con CVSS v4.0 de 9,2 y programó la corrección para el 21 de octubre de 2026 a las 14:00 UTC, 09:00 en Colombia. El aviso consultado todavía no detalla versiones afectadas ni corregidas.

NIVEL DE RIESGO

CRÍTICO

CERT-EU identifica los dos CVE siguientes y recoge una posible ejecución remota de código sin autenticación y afectación desde PHP 5. Son datos preliminares: no constituyen una confirmación técnica del fabricante ni prueban que toda instalación PHP sea explotable.

.

Vulnerabilidad identificada

CVE	PRODUCTOS AFECTADOS	SCORE CVSS	DESCRIPCIÓN	CISA KEV
CVE-2026-109618	PHP. Rango exacto pendiente de confirmación	**9,2 Crítica v4.0**	Posible RCE sin autenticación según CERT-EU. Mecanismo, CWE y vector CVSS completo no publicados en los avisos consultados.	**No verificado**
CVE-2026-109619	PHP. Rango exacto pendiente de confirmación	**9,2 Crítica v4.0**	Segundo fallo crítico. No se dispone de detalles para diferenciar sus condiciones de explotación de las del primer CVE	**No verificado**

¿Cómo se podrían explotar esta debilidad?

Escenario hipotético para priorización: Si se confirma una vía de RCE, un atacante podría alcanzar una aplicación expuesta y provocar ejecución no autorizada mediante el componente vulnerable. El impacto quedaría condicionado por la configuración y los permisos efectivos del servicio. No se conocen públicamente en los avisos consultados los requisitos ni el mecanismo de explotación

Acciones con los permisos del servicio: Si se confirma y materializa la ejecución remota de código, el atacante podría realizar operaciones con los privilegios del proceso PHP afectado. Esto no supone, por sí solo, obtener permisos de administrador o acceso completo al servidor.

Persistencia y ampliación del compromiso: Si el acceso obtenido permite escribir archivos o alcanzar otros recursos, podrían instalarse scripts maliciosos, como una web shell, o intentarse accesos a otros sistemas. Estas son consecuencias hipotéticas de una intrusión y no comportamientos confirmados para estas vulnerabilidades.



Impacto para Colombia y la región

- **Sectores afectados**: entidades de gobierno, salud, financiero, educación, comercio electrónico, telecomunicaciones y demás organizaciones que utilicen PHP en portales, aplicaciones o servicios digitales. La afectación dependerá de las versiones y configuraciones que confirme el fabricante.

- **Riesgo alto**: los servicios PHP expuestos a Internet deben priorizarse para evaluación y actualización. Si se confirma la ejecución remota de código sin autenticación, una explotación exitosa podría comprometer aplicaciones y recursos accesibles con los permisos del servicio afectado.

- **Posibles consecuencias**
  - Acceso no autorizado a información personal, financiera, comercial o institucional.
  - Alteración de páginas web, archivos de aplicaciones o datos.
  - Interrupción de portales, plataformas de comercio electrónico y servicios de atención al ciudadano.
  - Instalación de componentes maliciosos o persistencia, si los permisos obtenidos lo permiten.
  - Costos de investigación, recuperación y suspensión de operaciones, además de afectación reputacional.

- **Implicaciones en seguridad digital**
  - Identificar las aplicaciones PHP y sus responsables, incluidos servicios administrados por terceros.
  - Priorizar los activos expuestos a Internet y aquellos que procesen información sensible.
  - Coordinar con proveedores de hosting y tecnología la aplicación y verificación de las correcciones oficiales.
  - Preparar medidas de contención y recuperación para mantener la continuidad de los servicios críticos.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación de aplicación pública	**T1190**	Acceso inicial. Aplicaría si se confirma explotación de PHP a través de una aplicación accesible desde Internet. Asociación condicional al vector finalmente divulgado.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Intérprete de comandos y scripts	**T1059**	Ejecución. Hipótesis si, tras comprometer el servicio, se observa uso de intérpretes para ejecutar comandos. No implica que el fallo habilite una shell por sí mismo.
Componente de software de servidor — Web Shell	**T1505.003**	Persistencia. Hipótesis si se instala un script no autorizado para mantener acceso al servidor web. Requiere evidencia de escritura y uso; no se ha documentado aquí para estos CVE

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	DESCRIPCIÓN
Actualizar software (Update Software)	**M1051**	Medida principal. Aplicar la versión o paquete que el proveedor identifique expresamente como corregido para ambos CVE. Actualizar también imágenes y despliegues replicados. Confirmar el cambio en ejecución.
Segmentación de red	**M1030**	Separar los servidores PHP expuestos a Internet de los sistemas internos y restringir las comunicaciones a los servicios estrictamente necesarios. Cuando no sea posible aplicar la corrección de inmediato, evaluar el aislamiento temporal de las aplicaciones expuestas. Estas medidas reducen la exposición y el impacto potencial, pero no sustituyen la actualización.
Aislamiento de aplicaciones y sandboxing	**M1048**	Separar aplicaciones y recursos mediante entornos restringidos, contenedores o controles equivalentes, con permisos y montajes mínimos. El aislamiento limita impacto, pero no demuestra que el fallo sea inexplotable.
Gestión de cuentas privilegiadas	**M1026**	Evitar cuentas administrativas para ejecutar PHP y limitar acceso a secretos, bases de datos y tareas privilegiadas. Aplicar mínimo privilegio y revisar permisos efectivos de las cuentas de servicio.

Recomendaciones

- **Identificar y priorizar los activos** Elaborar un inventario de servidores, aplicaciones, servicios de alojamiento y contenedores que utilicen PHP. Registrar sus versiones, responsables y exposición a Internet, priorizando los sistemas públicos y aquellos que procesen información sensible.

- **Verificar las correcciones oficiales** Consultar los avisos de PHP y del proveedor de alojamiento o distribución para identificar las versiones o paquetes que corrigen CVE-2026-109618 y CVE-2026-109619. No considerar una instalación protegida únicamente por tener la última versión disponible antes del anuncio.

- **Aplicar la actualización con carácter prioritario** Desplegar las correcciones correspondientes tan pronto se confirme su disponibilidad. Coordinar pruebas de compatibilidad con los responsables de las aplicaciones y disponer de respaldos verificados y un procedimiento de recuperación.

- **Reducir temporalmente la exposición** Cuando no sea posible actualizar de inmediato, evaluar el aislamiento de las aplicaciones expuestas a Internet, conforme a la recomendación de CERT-EU. Restringir los accesos a los orígenes estrictamente necesarios, considerando el impacto sobre la continuidad del servicio.

- **Aplicar el principio de mínimo privilegio** limitar los permisos de las cuentas que ejecutan PHP, el acceso a archivos sensibles y las conexiones hacia bases de datos y otros sistemas. Estas medidas pueden reducir el impacto de una intrusión, pero no sustituyen la actualización.

- **Comprobar la cobertura de la actualización** verificar todas las instancias de PHP, incluidos PHP-FPM, módulos del servidor web, procesos de línea de comandos, contenedores y réplicas. Reiniciar o renovar los componentes cuando corresponda y validar el funcionamiento de las aplicaciones.

Fuentes

PHP Security Team — Upcoming Critical PHP Security Release, 20/10/2026
, disponible en:
https://www.php.net/archive/2026.php#2026-10-20-1

CERT-EU — Security Advisory 2026-018, versión inicial 21/10/2026
disponible en.
https://cert.europa.eu/publications/security-advisories/2026-018

PHP — Downloads and Installation Instructions
disponible en.
https://www.php.net/downloads.php

PHP – Upcoming Critical PHP Security Release
disponible en.
https://www.php.net/