



Alerta de seguridad global: Actualización crítica de PHP en Servidores de Hosting



Estimado cliente,

Nos comunicamos con usted para informarle sobre una alerta global de ciberseguridad emitida el día de **hoy, 21 de octubre de 2026**, que afecta al lenguaje de programación PHP (identificada bajo las vulnerabilidades **CVE-2026-109618** y **CVE-2026-109619**).

Al operar sus sitios web sobre nuestra infraestructura de servidores compartidos, VPS y Dedicados administrados, queremos transmitirle total tranquilidad: nuestro equipo de operaciones, en coordinación directa con nuestros proveedores de infraestructura perimetral, ya se encuentra ejecutando los protocolos de mitigación y parcheo correspondientes

A continuación, detallamos el plan de acción técnico y las validaciones requeridas de su parte:

Para neutralizar la vulnerabilidad sin interrumpir sus servicios, estamos aplicando una estrategia por etapas en nuestros nodos de datos:

1. **Despliegue de parches oficiales:** Estamos implementando de manera escalonada las actualizaciones nativas de PHP a las versiones seguras (8.2.35, 8.3.36, 8.4.27 y 8.5.12) en coordinación con las ventanas de mantenimiento de los centros de datos.
2. **Mitigación temporal de infraestructura (Alternativa inmediata):** Mientras se completan los reinicios de servicios individuales, hemos desactivado de forma preventiva las directivas globales `session.upload_progress` (vector principal del fallo) e incrementado la seguridad en las políticas de firewall perimetral. Esto bloquea el ataque antes de que llegue a su aplicación, permitiendo que su sitio web continúe operando de forma normal y segura.

La seguridad en entornos administrados requiere una acción coordinada. Para asegurar que su sitio web sea compatible con estas protecciones, le solicitamos realizar las siguientes revisiones:

- **Verifique e incremente su versión de PHP:** Ingrese a su panel de control Plesk. Si su sitio web está ejecutando *PHP 8.1* o *cualquier versión anterior* (como *PHP 7.4*), debe solicitar o programar la migración a *PHP 8.2* o *superior inmediatamente*. Las versiones *8.1* e inferiores han llegado al final de su vida útil y no reciben parches oficiales de seguridad.
- **Actualice aplicaciones y plugins corporativos:** Si aloja plataformas como WordPress, Laravel o sistemas de comercio electrónico, actualice el núcleo y todos los componentes a su última versión de inmediato. Los desarrolladores de software están lanzando actualizaciones críticas para asegurar que sus códigos no generen errores con los nuevos parches de memoria de los servidores.



Alerta de seguridad global: Actualización crítica de PHP en Servidores de Hosting



- **Evite modificaciones locales de configuración:** Le solicitamos encarecidamente no forzar la activación de parámetros como `session.upload_progress` o `session.auto_start` mediante archivos locales `.user.ini` o `.htaccess`, ya que esto anularía las protecciones perimetrales instaladas en el servidor

*** Nota importante de compatibilidad: ***

Al cambiar la versión de PHP, su sitio web se actualizará en pocos segundos. Le recomendamos abrir su página web en una pestaña de incógnito para verificar que todo cargue correctamente. Si nota algún error visual o de código (por incompatibilidad de su software antiguo con el nuevo PHP), puede regresar de inmediato a la pantalla anterior y volver a colocar la versión previa temporalmente mientras solicita a su diseñador web una revisión del código.

Es posible que durante las próximas horas observe micro-cortes intermitentes de pocos segundos en el servicio web mientras los servidores aplican las actualizaciones de los componentes principales. No se requiere ninguna acción por su parte durante estos procesos

Agradecemos su confianza mientras aseguramos la continuidad y protección de su negocio en la nube.

Cualquier comentario estamos para servirle en nuestro [portal de tickets](#) o por el correo soporte@irivinsu.com

Atentamente,

IRIVINSU