Buenos Aires, 22 oct. 2026

A nuestros clientes y partners,

Fieles a nuestro compromiso de brindar los máximos niveles de seguridad posibles a nuestros clientes, esta comunicación oficial tiene como objetivo ofrecer detalles y garantías sobre las medidas adoptadas para honrar dicho compromiso sobre las recientes vulnerabilidades críticas divulgadas por la PHP Foundation junto con OpenAI y otras firmas de seguridad nativas de IA.

Resumen ejecutivo y cronología

Nota 1: el producto **InvGate Service Management** se denominará **IGSM** en el resto del documento

Nota 2: todas las horas están expresadas en UTC.

- El 20 de octubre de 2026, el proyecto PHP publicó un aviso de seguridad sobre dos vulnerabilidades críticas, **CVE-2026-109618** y **CVE-2026-109619**, ambas con una puntuación CVSS de 9,2/10 (puntuación con la que InvGate coincide y que utiliza como calificación interna oficial). El equipo de Seguridad de InvGate tomó conocimiento de ellas y comenzó los preparativos para desplegar los parches al día siguiente.
- El 21 de octubre de 2026 a las 12:00, el equipo de Seguridad comenzó los preparativos a partir de detalles filtrados encontrados en redes sociales especializadas en seguridad de la información.
- A las 12:30 (antes la comunicación oficial por parte de la PHP Foundation, a las 14:00), InvGate comenzó a evaluar el impacto del despliegue del parche sobre la continuidad del negocio; la conclusión fue que durante el proceso de parcheo no habría tiempo de indisponibilidad visible para los clientes.
- Entre las 13:55 y las 15:10, el equipo de Seguridad comenzó a desplegar las medidas de mitigación adaptadas a los detalles técnicos filtrados de las vulnerabilidades, además de crear alertas en el SIEM basadas en los indicadores de compromiso filtrados, para minimizar y disuadir posibles intentos de explotación antes y durante la ventana de despliegue del parche.
- A las 16:50, el equipo de Infraestructura lideró el proceso de parcheo en los entornos de los clientes, que consistió principalmente en **actualizar las**

versiones vulnerables de PHP a PHP v8.4.27 en todos los clústeres de IGSM de los entornos de producción, desarrollo y control de calidad (QA) alojados en nuestro entorno cloud, y publicar nuevos paquetes de instalación para los clientes on-premise.

- Entre las 17:00 y las 22:30, se completaron con éxito las siguientes tareas:
    - Despliegue de la versión actualizada de PHP en todos los clústeres de IGSM
    - Identificación y parcheo de la infraestructura específica de clientes que resultó afectada
    - Creación y publicación en releases.invgate.com de los paquetes on-premise de IGSM con la versión actualizada de PHP
    - Monitoreo continuo de la disponibilidad y de los eventos de seguridad en los clústeres actualizados
    - Comunicaciones generales y específicas a los clientes, a cargo del equipo de Soporte.

Productos afectados

- InvGate Service Management (IGSM)
    - Versiones SaaS
    - Versiones on-premise: v8.25.2 y anteriores
- InvGate SSO Provider on-premise
- Integraciones a medida de clientes que funcionan sobre PHP

Productos y servicios no afectados

- InvGate Asset Management (IGAM)
- InvGate Connector, tanto en despliegues de IGSM como de IGAM

Remediación técnica

La primera de las medidas preventivas fue limitar de forma estricta la tasa de solicitudes (rate limiting) de todos los endpoints que admiten los métodos HTTP

POST/PUT/PATCH en nuestro Web Application Firewall, ya que las filtraciones públicas de los detalles de las vulnerabilidades nos permitieron determinar, con un alto grado de confianza, que se trataba de vulnerabilidades basadas en corrupción de memoria. La segunda medida fue deshabilitar temporalmente y reducir los valores de la familia de variables **session.upload_progress** de PHP, **upload_max_filesize** y **max_file_uploads**, respectivamente, para reducir la probabilidad de explotación antes de la liberación del parche y durante la ventana de aplicación del mismo. Todo esto se realizó primero en recursos internos de staging y, una vez validado, se desplegó en la infraestructura de producción.

Una vez liberado el parche, alrededor de las 13:45, los equipos de Infraestructura y Seguridad iniciaron el despliegue del mismo y la publicación de las nuevas versiones. Fue un proceso de tres partes: primero, actualizar los repositorios de seguridad del sistema operativo de las instancias EC2 para obtener y descargar el paquete de PHP v8.4.27 y luego desplegarlo en toda la flota EC2 como parte de un procedimiento de liberación de emergencia. La segunda parte del proceso, en paralelo con la primera, consistió en generar nuevos instaladores de IGSM para Windows y Linux para los clientes on-premise de InvGate, que terminarían publicándose en releases.invgate.com. La tercera y última parte del proceso consistió en volver a desplegar todos los entornos en la nube de IGSM para que utilicen la nueva versión de PHP, v8.4.27, y en monitorear posibles caídas y problemas que pudieran surgir; no hubo ninguno. Todas las limitaciones temporales se revirtieron una vez que toda la flota de clústeres de IGSM estuvo actualizada a la versión de PHP mencionada.

Toda la investigación y las acciones paliativas se realizaron en base a los siguientes avisos oficiales: PHP, Wiz y Calif.io. Se utilizaron herramientas internas basadas en Terraform para verificar y desplegar la versión actualizada de PHP en todos los clústeres de IGSM.

Monitoreo de la situación

Nuestro equipo de Seguridad analizó los logs de las aplicaciones y del sistema operativo, y la telemetría de EDR, a través de nuestro SIEM para detectar tanto intentos como explotaciones exitosas; nos complace informar que **no se encontró explotación activa de estas vulnerabilidades de PHP entre el 17 y el 21 de octubre**

de 2026; nuestro compromiso es seguir monitoreando la situación e incorporar a nuestras alertas de SIEM y a las reglas de detección de EDR los nuevos indicadores de compromiso y las nuevas tácticas, técnicas y procedimientos (TTP) que se descubran.

Además, el equipo de Seguridad analizó tanto los logs de la aplicación IGSM como los de PHP en busca de evidencia de corrupción de memoria, monitoreó alertas vinculadas con la ejecución no interactiva de código o comandos por parte de herramientas de exfiltración, toma de control y comunicación de uso común, y realizó un barrido completo de actividad sospechosa a nivel de sistema operativo en toda la flota de clústeres de IGSM.

Notificación a los clientes y seguimiento

Una vez confirmado el éxito del proceso de parcheo, nuestro equipo de Soporte notificó a los clientes y partners afectados, tanto en la nube como on-premise, con los resultados de este proceso. El despliegue de las acciones preventivas, las pruebas y el parcheo en staging y producción, la creación y publicación de los instaladores y la notificación a los clientes **se realizaron a lo largo de diez horas y media** (de 12:00 a 22:30 UTC) el 21 de octubre de 2026.

Pasos de mitigación para clientes SaaS y on-premise

A continuación se detallan las acciones que deben seguir nuestros clientes, según el tipo de despliegue de IGSM que corresponda.

- **Despliegue SaaS de IGSM:** la actualización del servicio administrado por InvGate ya fue aplicada, por lo que no se requiere ninguna acción para el servicio en la nube.
- **Despliegues on-premise en Windows**: instalar la última actualización publicada de InvGate Service Management.
- **Despliegues on-premise en Linux:** aplicar la actualización de seguridad de PHP de su proveedor de sistema operativo. PHP no está incluido en el paquete de InvGate para Linux

- **SSO Provider de IGSM o componentes específicos del cliente:** seguir las indicaciones del equipo de Soporte de InvGate para su despliegue on-premise. Si su infraestructura personalizada está alojada en un entorno productivo en la nube de InvGate, ya fue actualizada con éxito.

El equipo de Soporte de InvGate notificará de inmediato a los clientes si cambia el resultado de nuestras verificaciones internas de seguridad en curso y los clientes resultan afectados, en cumplimiento de nuestras políticas internas de seguridad y de las leyes de protección de datos regionales o específicas de cada país, como GDPR, LGPD y otras.

Si necesita ayuda para confirmar los próximos pasos o tiene consultas sobre la respuesta de InvGate y el manejo de esta operación de seguridad, contacte a nuestro equipo de Soporte en https://support.invgate.com; estamos para ayudarle con todas sus consultas y necesidades.