invgate

Buenos Aires, 22 out. 2026

Aos nossos clientes e parceiros,

Fiéis ao nosso compromisso de oferecer os mais altos níveis possíveis de segurança aos nossos clientes, esta comunicação oficial sobre as recentes vulnerabilidades críticas divulgadas pela PHP Foundation, juntamente com a OpenAI e outras empresas de segurança nativas de IA, tem como objetivo fornecer detalhes e garantias sobre as medidas adotadas para honrar esse compromisso.

Resumo executivo e cronologia

Nota 1: o produto **InvGate Service Management** será chamado de **IGSM** no restante do documento

Nota 2: todos os horários estão em UTC.

- Em 20 de outubro de 2026, o projeto PHP publicou um aviso de segurança sobre duas vulnerabilidades críticas, **CVE-2026-109618** e **CVE-2026-109619**, ambas com pontuação CVSS de 9,2/10 (pontuação com a qual a InvGate concorda e que adota como classificação interna oficial). A equipe de Segurança da InvGate tomou conhecimento delas e iniciou os preparativos para a implantação do patch no dia seguinte.
- Em 21 de outubro de 2026, às 12:00, a equipe de Segurança iniciou os preparativos defensivos com base em detalhes vazados encontrados em redes sociais especializadas em segurança da informação.
- Às 12:30 (antes do fim do embargo pela PHP Foundation, às 14:00), a InvGate começou a avaliar o impacto da implantação do patch na continuidade dos negócios; a conclusão foi que não haveria indisponibilidade perceptível para os clientes durante o processo de aplicação do patch.
- Entre 13:55 e 15:10, a equipe de Segurança começou a implantar medidas defensivas adaptadas aos detalhes técnicos vazados das vulnerabilidades, além de criar alertas no SIEM baseados nos indicadores de comprometimento vazados, para minimizar e dissuadir possíveis tentativas de exploração antes e durante a janela de implantação do patch.
- Às 16:50, a equipe de Infraestrutura liderou o processo de aplicação do patch nos ambientes dos clientes, que consistiu principalmente em **atualizar as**

versões vulneráveis do PHP para o PHP v8.4.27 em todos os clusters do IGSM nos ambientes de produção, desenvolvimento e QA hospedados em nosso ambiente em nuvem, e publicar novos pacotes de instalação para clientes on-premise.

- Entre 17:00 e 22:30, as seguintes tarefas foram concluídas com sucesso:
  - Implantação da versão atualizada do PHP em todos os clusters do IGSM
  - Identificação e aplicação de patch na infraestrutura específica de clientes que foi afetada
  - Criação e publicação em releases.invgate.com dos pacotes on-premise do IGSM com a versão atualizada do PHP
  - Monitoramento contínuo da disponibilidade e dos eventos de segurança nos clusters atualizados
  - Comunicações gerais e direcionadas aos clientes, conduzidas pela equipe de Suporte.

Produtos afetados

- InvGate Service Management (IGSM)
  - Versões SaaS
  - Versões on-premise: v8.25.2 e anteriores
- InvGate SSO Provider on-premise
- Integrações sob medida para clientes executadas em PHP

Produtos e serviços não afetados

- InvGate Asset Management (IGAM)
- InvGate Connector, tanto em implantações do IGSM quanto do IGAM

Correção técnica

A primeira das medidas preventivas foi limitar rigorosamente a taxa de requisições (rate limiting) de todos os endpoints que aceitam os métodos HTTP **POST**/**PUT**/**PATCH** em nosso Web Application Firewall, já que os vazamentos públicos dos detalhes das vulnerabilidades nos permitiram determinar, com alto grau de

confiança, que elas eram baseadas em corrupção de memória. A segunda medida foi desabilitar temporariamente e reduzir os valores da família de variáveis **session.upload_progress** do PHP, **upload_max_filesize** e **max_file_uploads**, respectivamente, para reduzir a probabilidade de exploração antes do fim do embargo e durante a janela de aplicação do patch. Tudo isso foi realizado primeiro em recursos internos de staging e, após a validação, foi implantado na infraestrutura de produção.

Quando o embargo foi levantado, por volta das 13:45, as equipes de Infraestrutura e Segurança iniciaram a aplicação do patch e os processos de publicação das novas versões. Foi um processo em três partes: primeiro, atualizar os repositórios de segurança do sistema operacional das instâncias EC2 para obter e baixar o pacote do PHP v8.4.27 e, em seguida, implantá-lo em toda a frota EC2 como parte de um procedimento de liberação de emergência. A segunda parte do processo, em paralelo com a primeira, foi gerar novos instaladores do IGSM para Windows e Linux para os clientes on-premise da InvGate, que seriam publicados em releases.invgate.com. A terceira e última parte do processo foi reimplantar todos os ambientes SaaS do IGSM para que usassem a nova versão do PHP, v8.4.27, e monitorar eventuais quedas e problemas que pudessem surgir; não houve nenhum. Todas as limitações temporárias foram revertidas assim que toda a frota de clusters do IGSM foi atualizada para a versão do PHP mencionada.

Toda a investigação e as ações paliativas foram realizadas com base nos seguintes avisos oficiais: PHP, Wiz e Calif.io. Ferramentas internas baseadas em Terraform foram utilizadas para verificar e implantar a versão atualizada do PHP em todos os clusters do IGSM.

Monitoramento da situação

Nossa equipe de Segurança analisou os logs de aplicação e do sistema operacional e a telemetria de EDR por meio do nosso SIEM, para detectar tanto tentativas quanto explorações bem-sucedidas; temos o prazer de informar que **nenhuma exploração ativa dessas vulnerabilidades do PHP foi encontrada entre 17 e 21 de outubro de 2026**; nosso compromisso é continuar monitorando a situação e incorporar aos nossos alertas de SIEM e às regras de detecção de EDR os novos indicadores de

comprometimento e as novas táticas, técnicas e procedimentos (TTPs) que forem descobertos.

Além disso, a equipe de Segurança analisou tanto os logs da aplicação IGSM quanto os do PHP em busca de evidências de corrupção de memória, monitorou alertas ligados à execução não interativa de código ou comandos por ferramentas de exfiltração, tomada de controle e comunicação de uso comum, e realizou uma varredura completa de atividades suspeitas no nível do sistema operacional em toda a frota de clusters do IGSM.

Notificação aos clientes e acompanhamento

Depois de confirmado o sucesso do processo de aplicação do patch, nossa equipe de Suporte notificou os clientes e parceiros afetados, tanto SaaS quanto on-premise, com atualizações sobre esse processo bem-sucedido. A implantação das ações preventivas, os testes e a aplicação do patch em staging e produção, a criação e publicação dos instaladores e a notificação aos clientes **foram realizados ao longo de dez horas e meia** (das 12:00 às 22:30 UTC) em 21 de outubro de 2026.

Etapas de mitigação para clientes SaaS e on-premise

Abaixo estão as ações que os clientes devem seguir, de acordo com o tipo de implantação do IGSM aplicável.

- **Implantação SaaS do IGSM:** a atualização do serviço gerenciado pela InvGate já foi aplicada, portanto nenhuma ação é necessária para o serviço principal em nuvem
- **Implantações on-premise no Windows**: instalar a última atualização publicada do InvGate Service Management
- **Implantações on-premise no Linux:** aplicar a atualização de segurança do PHP do fornecedor do seu sistema operacional. O PHP não está incluído no pacote da InvGate para Linux
- **SSO Provider do IGSM ou componentes específicos do cliente:** seguir as orientações do Suporte da InvGate para a sua implantação on-premise. Se a sua infraestrutura personalizada estiver hospedada na infraestrutura de produção da InvGate, ela já foi atualizada com sucesso.

A equipe de Suporte da InvGate notificará imediatamente os clientes se o resultado das nossas verificações internas de segurança em andamento mudar e os clientes forem afetados, em conformidade com nossas políticas internas de segurança e com as leis de proteção de dados regionais ou específicas de cada país, como GDPR, LGPD e outras.

Se precisar de ajuda para confirmar os próximos passos ou tiver dúvidas sobre a resposta da InvGate e o tratamento desta operação de segurança, entre em contato com nossa equipe de Suporte em https://support.invgate.com; estamos aqui para ajudar com todas as suas dúvidas e necessidades.