invgate

Buenos Aires, October 22, 2026

To our clients and partners,

Following our commitment to provide the utmost possible security levels to our customers, this official communication about the recent critical vulnerabilities disclosed by the PHP Foundation alongside OpenAI and other AI-first security firms aims to provide details and assurance about the steps taken to honor said commitment.

Executive summary and timeline

Notes: the **InvGate Service Management** product will be referred to as **IGSM** for the rest of the document

Note 2: all timestamps are in UTC.

- On October 20, 2026 the PHP project released an advisory for two critical vulnerabilities, **CVE-2026-109618** and **CVE-2026-109619**, both with a CVSS score of 9.2/10 (to which score InvGate agrees and uses as internal official score). InvGate's Security team became aware of them and started preparations for the patch rollout to be done the next day.
- On October 21, 2026 at 12:00 PM, the Security team started defensive preparations based on leaked details found on specialized InfoSec social media
- At 12:30 PM (before the 2:00 PM embargo lift by the PHP Foundation), InvGate started assessing the impact of the patch rollout on business continuity; conclusion was there would be no customer-facing downtime during the patching process.
- Between 1:55 and 3:10 PM, the Security team started deploying defensive measures tailored to the vulnerabilities' leaked technical details as well as creating SIEM alerts tailored to the leaked Indicators of Compromise, to minimize and deter possible exploitation attempts before and during the patch rollout window.
- At 4:50 PM, the Infrastructure team spearheaded the patching process across customer environments, which consisted mainly of **updating the vulnerable PHP versions to PHP v8.4.27 across all IGSM clusters on Production,**

Development and QA environments hosted in our cloud environment, and publishing new installation packages for on-premise customers.

- Between 5:00 and 10:30 PM, the following tasks were successfully completed:
    - PHP updated version patch rollout across all IGSM clusters
    - Identification and patching of customer-specific affected infrastructure
    - IGSM on-prem packages creation and publishing to releases.invgate.com with the updated PHP version
    - Constant availability and security events monitoring across the updated clusters
    - General and targeted customer communications, handled by the Support team.

Impacted products

- InvGate Service Management (IGSM)
    - SaaS versions
    - On-prem versions: v8.25.2 and below
- InvGate on-prem SSO Provider
- Customer-tailored integrations running on PHP

Not impacted products and services

- InvGate Asset Management (IGAM)
- InvGate Connector on either IGSM or IGAM deployments

Technical remediation

The first of the preventive measures was to heavily rate-limit all endpoints supporting the **POST**/**PUT**/**PATCH** HTTP methods on our Web Application Firewall, since public leaks of the vulnerabilities' details allowed us to determine with a high confidence degree the vulnerabilities were memory corruption-based. The second measure was to temporarily disable and decrease the values of the **session.upload_progress** PHP global variables family, **upload_max_filesize** and **max_file_uploads**, respectively, to reduce the exploitation probabilities before the embargo lift and during the patching window. All this was performed on staging internal resources, and, upon validation, it was deployed on production infrastructure.

Once the embargo was lifted around 1:45 PM, the Infrastructure and Security teams started the patch rollout and new version release processes. This was a threefold process: first, updating the EC2 instances' OS security repositories to obtain and download the v8.4.27 PHP package, then deploying it across the EC2 fleet as part of an emergency release procedure. The second part of the process, at the same time as the first, was to produce new IGSM installers for Windows and Linux for InvGate's on-prem customers, which would end in publishing them at releases.invgate.com. The third and last part of the process was to redeploy all the IGSM SaaS environments to use the newly updated PHP version, v8.4.27, and to monitor for downtime and arising issues; there were none. All temporary limitations were reverted once the entire IGSM clusters fleet was updated to the aforementioned PHP version.

All research and palliative actions were performed based on the following official advisories: PHP, Wiz and Calif.io. Internal tooling based on Terraform was used to check and deploy the updated PHP version across all IGSM clusters.

Situational monitoring

Our Security team analyzed application and OS logs and EDR telemetry via our SIEM to detect both attempts and successful exploitation; we're happy to inform that **no exploitation of these PHP vulnerabilities was found to be active between October 17 and October 21, 2026**; our commitment is to continue monitoring the situation, and to add newly discovered Indicators of Compromise and Tactics, Techniques and Procedures (TTPs) to our SIEM alerts and EDR detection rulesets.

Moreover, the Security team analyzed logs for memory corruption evidence on both IGSM application and PHP logs, monitored alerts tied to non-interactive code/commands execution of commonly used exfiltration/takeover/communication tools, and produced a complete sweep of suspicious OS-based activity across the entire IGSM clusters fleet.

Customer notification and follow-ups

After the patching process was confirmed to be successful, our Support team notified affected SaaS and on-prem customers and partners with updates about this successful process. The preventive actions deployment, stage and production testing and patching, installers creation and publishing and customer notification **processes were performed across ten and a half hours** (12:00 to 10:30 PM UTC) on October 21, 2026.

Mitigation steps for SaaS and on-premise customers

Follow-up actions for our customers are listed below, depending on the applicable IGSM deployment.

- **IGSM SaaS deployment:** the update to the InvGate-managed service has been applied, so no action is required for the core Cloud service
- **On-premise Windows deployments**: install the latest published InvGate Service Management update
- **On-premise Linux deployments:** apply your operating system vendor's PHP security update. PHP is not bundled with InvGate's Linux package
- **IGSM SSO Provider or customer-specific components:** follow the guidance provided by InvGate Support for your on-prem deployment. If your custom infrastructure is hosted on InvGate's production infrastructure, it has been successfully updated.

InvGate's Support team will promptly notify customers if the outcome of our ongoing internal security checks changes and customers are affected, in compliance with our internal security policies and regional or country-specific data privacy laws such as GDPR, LGPD and others.

If you need help either confirming your next steps or have follow-up questions about InvGate's response and handling of this security operation, contact our Support team at https://support.invgate.com; we're here to help you with all your questions and needs.