TECHNICAL DEBRIEF

Security update · PHP2Shell

PHP2Shell: technical debrief

What happened, how we have responded, and where we are now.

ISSUED	PREPARED FOR	STATUS
22 October 2026	OpenCRM customers	Patched; review complete, no signs of attack found

01 Summary

Two critical vulnerabilities in PHP, the programming language our platform runs on, were leaked on the evening of 20 October 2026, ahead of their planned disclosure. Known as **PHP2Shell**, they allow an attacker to take control of a web server with a single request, without logging in. PHP rates both flaws 9.2 out of 10 on the CVSS v4.0 severity scale, and attacks across the internet began before an official fix was available. We have found no evidence that OpenCRM was targeted or received any attack.

On 21 October we put protective measures in place at the web server and in the PHP configuration, following PHP's own interim guidance. These reduce the likelihood of an attack considerably. PHP is clear that interim measures are partial and only a patched version removes the flaws. PHP made its fixes available on the afternoon of 21 October. Our team then worked through the night to build, test and roll out a patched version to all customer systems, removed the interim measures once each system was patched, and increased our monitoring. We have also completed our review of activity since the leak, which confirmed there were no signs of attack.

> **WHERE WE ARE NOW**
>
> The patched version is now in place on customer systems. We have reduced our risk rating from **Critical** to **Low**. Our review of activity since 20 October is complete and found no signs of attack. We continue to monitor closely and will tell affected customers directly if that changes.

02 What happened

Details of the two flaws leaked before PHP's planned disclosure and security firms quickly confirmed they were real. The timeline below is drawn from public sources and shown in UTC.

Date (UTC)	Event
20 Oct (evening)	Details leak. PHP announces an emergency release and security firms confirm the flaws are real.
21 Oct, 02:13	A PHP core developer states that only patching fully fixes the flaws.
21 Oct, 07:43	Cloudflare reports early attacks against PHP sites across the internet.
21 Oct, c. 14:00	PHP releases fixes for its current versions (8.2 to 8.5), plus limited source-level patches for some older versions for organisations that build PHP themselves.
21 Oct	OpenCRM puts protective measures in place and starts work on a patched version.
21–22 Oct (overnight)	OpenCRM's team works through the night to build, test and roll out the patched version to all customer systems.
22 Oct	OpenCRM completes its review of activity since 20 October and finds no signs of attack.

The two flaws work differently:

CVE-2026-109618	A specially crafted upload request can cause PHP to run out of memory part-way through reading it, corrupting its internal state. This is the main confirmed attack route.
CVE-2026-109619	Data left behind by one request can be reused by a later request. PHP's confirmed attack paths depend on how a server runs PHP.

03 How this affects OpenCRM

- **What is at stake.** Our servers host customer CRM instances. A successful attack could expose the data of more than one customer at once, and could carry notification duties under UK GDPR.
- **Why it is urgent.** The attack needs no login and works against default PHP settings. Mass scanning of the internet for vulnerable servers is expected.
- **Our commitment.** If we find evidence that customer data has been affected, we will notify the customers concerned without undue delay.

04 What we have done

We layered several measures across our hosting environments, following PHP's interim advice. The request filtering and configuration changes were temporary and were removed once each system was patched.

Measure	What it does
Patched version of PHP	Applies the PHP security team's official patch, removing the flaws at source. Now in place on all customer systems.
Request filtering at the web server	Rejects the upload-style requests used by the main confirmed attack route before they reach PHP, while legitimate OpenCRM functions continue to work.
PHP configuration hardening	Changes PHP's runtime settings, as PHP recommends, to narrow the confirmed attack paths for both flaws.
Enhanced logging and monitoring	Detailed logging of relevant requests, plus frequent automated checks for signs of attack or unexpected change. Continuing.
Review of activity since the leak	A check of server and error logs, crash records and file integrity against known-good code for the period since 20 October. Complete: no signs of attack found.

05 Risk position

The protective measures reduce the likelihood of a break-in. Only a patched version of PHP removes the flaw itself. The impact of a successful attack stays severe throughout.

Stage	Likelihood	Impact	Overall risk
Before protective measures (morning of 21 Oct)	Very high: no fix available, attacks under way, no login needed	Severe	**Critical**
After protective measures, before the patch	Medium: known attack routes narrowed, but PHP confirms the measures are partial	Severe	**Medium**
Now: patched version in place	Low: flaw removed at source	Severe	**Low**

These ratings reflect our completed review, which found no signs of attack. They will change only if new information emerges.

06 What happens next

1. **Patched version of PHP (complete).** Our team worked through the night to build the patched version from the PHP security team's official patch, test it and roll it out to all customer systems.

2. **Monitoring and logging (ongoing).** We are recording relevant requests and running frequent automated checks so that any attack is detected quickly.

3 **Review of activity since the leak (complete).** The review found no signs of attack. If anything is found later, the affected server is treated as a security incident and affected customers are contacted.

4 **Further hardening (under review).** We are considering additional hardening for the hosting environment and will apply what adds protection without affecting service.

07 Residual risks

We want to be open about what remains, even once the planned steps are complete.

- **We keep watching.** Our review found no signs of attack. No review can rule out every possibility, so we continue to monitor closely.
- **Impact would be serious.** A successful attack would give an attacker control of the affected server, which is why we are acting at this pace.

WHAT THIS MEANS FOR YOU

Our review is complete and found no signs of attack, so we are not asking customers to take any action. If anything changes, we will contact you directly and tell you what to do.

Questions? Contact the OpenCRM support team on +44 (01748) 473000 or at support@opencrm.co.uk.

PUBLIC SOURCES

- BleepingComputer: PHP ships emergency patches for critical PHP2Shell flaws
- Sansec: Critical PHP RCE, CVE-2026-109618 and CVE-2026-109619
- ma.ttias.be: How to apply the patches
- Teramont: PHP2Shell patch status and hosting guide

Basis of note: OpenCRM's risk assessment of 21 October 2026, updated on 22 October 2026 for the patch rollout and completed review, and the public sources above. Risk ratings are OpenCRM's own assessment and may change as our review progresses. Some technical detail is deliberately withheld to protect the security of our environment.