

PHP Critical Vulnerabilities (CVE-2026-109618 and CVE-2026-109619) and rConfig

CRITICAL

Advisory ID	rCFG-SA-2026-01
First Published	20 October 2026, 20:33:27
Last Updated	21 October 2026, 15:47 IST
Version	0.9 (Interim)
Status	Investigating
Workarounds	Network isolation and PHP configuration changes (see Workarounds)
Affected component	PHP runtime
CVE	CVE-2026-109618, CVE-2026-109619
CVSS Score	9.2 (per CERT-EU). CVSS v4 vector from the PHP project: CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

All times are Irish Standard Time (IST, UTC+1).

Summary

- The PHP project released PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 on 21 October 2026. They fix two critical vulnerabilities, CVE-2026-109618 (RCE via OOM corruption, GHSA-w8hw-w9fx-j79w) and CVE-2026-109619 (RCE via stale global state, GHSA-6wmf-4rv5-p3rp), both of which can allow unauthenticated remote code execution.
- The PHP project says all PHP installations serving web requests are at risk, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed, with the highest risk for mod_php. It states that updating is the only complete solution.
- These are vulnerabilities in PHP, not in rConfig’s own code. rConfig runs on PHP, so the fix is to update PHP on the server that hosts it. We are testing each rConfig version against the fixed PHP releases and will update this advisory as findings are confirmed.
- Update PHP on the host running rConfig as soon as the fixed version is available from your package source, and keep rConfig off the public internet until then.

What is known, and how sure we are

Every statement is labelled: Confirmed means stated by the PHP Foundation or CERT-EU; Reported means relayed second-hand and not verified; Unknown means nothing reliable is public.

ITEM	DETAIL	CONFIDENCE
CVE IDs	CVE-2026-109618 (GHSA-w8hw-w9fx-j79w) and CVE-2026-109619 (GHSA-6wmf-4rv5-p3rp)	Confirmed (PHP project, CERT-EU)
CVSS	9.2 for both (CERT-EU). CVSS v4 vector published by the PHP project for CVE-2026-109619	Confirmed (CERT-EU, PHP project)
Impact	Unauthenticated remote code execution, demonstrated by the PHP project against mod_php and PHP-FPM. Highest risk for mod_php, where an unauthenticated request can trigger the attack before any application code runs	Confirmed (PHP project)
Affected PHP versions	All PHP installations serving web requests before 8.2.35, 8.3.36, 8.4.27 and 8.5.12. PHP 8.1 and older no longer receive updates from the PHP project, which provided minimal source backports for 7.4, 8.0 and 8.1. CERT-EU's report about all versions from PHP 5 onwards remains unverified	Confirmed (PHP project)
Fixed versions	PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12, released 21 October 2026	Confirmed (PHP project)
Exploitation	The PHP advisory describes the issue technically. No exploitation reported by CERT-EU at the time of its advisory	Confirmed (PHP project, CERT-EU)

Affected products

Vulnerable products

These are vulnerabilities in PHP, not in rConfig's own code. Any rConfig installation running on an affected PHP version is exposed through PHP. Until the PHP version on your server is updated, treat the installation as potentially exposed.

rConfig runs on the PHP version installed on your own server, so exposure depends on that version. The tables below map each rConfig release to the PHP versions it runs on, taken from its composer.json and composer.lock, and to the fixed PHP release identified for those versions. If you run rConfig Pro 7 or rConfig Core from February 2024 onwards, check the version in your composer.json and map it to the tables. No rConfig release is confirmed vulnerable or not vulnerable yet; the tables are updated as we test each one.

rConfig Pro

PRO VERSION	LAST RELEASE DATE	PHP IT RUNS ON	RECOMMENDED ACTION
6.0 to 6.3	2022-05 to 2022-07	8.0, 8.1	PHP 8.1 and older no longer receive updates from the PHP project. Use a vendor backport, build from source with the PHP security team's backport, or upgrade to a supported PHP version. Restrict access and contact us before changing PHP

PRO VERSION	LAST RELEASE DATE	PHP IT RUNS ON	RECOMMENDED ACTION
6.4 to 6.7	2022-07 to 2023-01	8.1	PHP 8.1 and older no longer receive updates from the PHP project. Use a vendor backport, build from source with the PHP security team's backport, or upgrade to a supported PHP version. Restrict access and contact us before changing PHP
6.8	2023-03	8.1, 8.2	Update PHP to 8.2.35 once available from your package source
6.9	2023-07	8.1, 8.2	Update PHP to 8.2.35 once available from your package source
6.11	2024-01	8.2, 8.3	Update PHP to 8.2.35 or 8.3.36 once available from your package source
7.0 to 7.2	2024-06 to 2025-01	8.2, 8.3	Update PHP to 8.2.35 or 8.3.36 once available from your package source
7.3	2025-03	8.2, 8.3, 8.4	Update PHP to 8.2.35 or 8.3.36 or 8.4.27 once available from your package source
8.0	2025-12	8.3, 8.4	Update PHP to 8.3.36 or 8.4.27 once available from your package source
8.1	2026-04	8.4	Update PHP to 8.4.27 once available from your package source
8.2	2026-07	8.4	Update PHP to 8.4.27 once available from your package source
8.3	2026-09	8.4, 8.5	Update PHP to 8.4.27 or 8.5.12 once available from your package source
8.4	2026-10	8.4, 8.5	Update PHP to 8.4.27 or 8.5.12 once available from your package source

rConfig Core

CORE VERSION AND PERIOD	MINIMUM PHP (COMPOSER.LOCK)	RECOMMENDED ACTION
6.0.0-core, Mar 2023 to Feb 2024	8.1	PHP 8.1 and older no longer receive updates from the PHP project. Use a vendor backport, build from source with the PHP security team's backport, or upgrade to a supported PHP version. Restrict access and contact us before changing PHP
6.0.0-core, Feb 2024	8.2	Update PHP to 8.2.35 once available from your package source
6.0.0-core, Sep 2024	8.2	Update PHP to 8.2.35 once available from your package source

CORE VERSION AND PERIOD	MINIMUM PHP (COMPOSER.LOCK)	RECOMMENDED ACTION
8.0.0, Oct 2024	8.2	Update PHP to 8.2.35 once available from your package source
8.0.0, Oct 2025 (Laravel 12 upgrade)	8.3	Update PHP to 8.3.36 once available from your package source
8.0.0, Apr 2026	8.4	Update PHP to 8.4.27 once available from your package source

Products confirmed not vulnerable

No rConfig release is confirmed not vulnerable at this time.

Workarounds

- Updating PHP is the only complete solution. The measures below reduce exposure to specific attack paths but do not make an installation safe.
- If you have not already, restrict access to rConfig immediately, ideally to a VPN or trusted management IP addresses. Do not expose the web interface directly to the internet.
- CVE-2026-109618 (OOM corruption): set `memory_limit=-1` in a way applications cannot override (for example `php_admin_value` in the FPM pool or Apache configuration) and check that nothing puts a finite limit back. Set a low `post_max_size` (8M if you do not need file uploads, 32M if you do) and keep `upload_max_filesize` below it. Use a container or cgroup limit as an availability boundary. Do not use `RLIMIT_AS` or `RLIMIT_DATA`.
- CVE-2026-109619 (stale global state): set `session.upload_progress.enabled=0` and restart every PHP worker, using `php.ini`, an FPM pool or server configuration that applies before request parsing. On PHP 8.5, also set `fatal_error_backtraces=0`.
- As a precaution rConfig has taken enterprise-demo, msp-demo, isp-demo, edu-demo, sme-demo (rconfig.com), crm.rconfig.com and the portal out of service. All seven hostnames now redirect to www.rconfig.com.

Fixed software

The PHP project released the fixed versions below on 21 October 2026. The remedy is to update PHP on the host running rConfig. Linux distributions and LTS vendors received the patches in advance, so check your vendor for updated packages. Third-party repositories can take longer.

PRODUCT	FIRST FIXED RELEASE
PHP 8.2	8.2.35 (replaces 8.2.34). PHP 8.2 reaches end of life on 31 December 2026
PHP 8.3	8.3.36 (replaces 8.3.35)
PHP 8.4	8.4.27 (replaces 8.4.26)
PHP 8.5	8.5.12 (replaces 8.5.11)

PRODUCT	FIRST FIXED RELEASE
PHP 8.1 and older	No update from the PHP project. Use a vendor backport, build from source with the PHP security team's backport (provided for 7.4, 8.0 and 8.1), or upgrade to a supported version
rConfig	These are PHP vulnerabilities, so the fix is a PHP update on your server. We are testing each rConfig version against the fixed PHP releases

How to update PHP: download the fixed release or find your operating system's package from the PHP project's downloads page. [PHP downloads](https://www.php.net/downloads.php) (https://www.php.net/downloads.php)

Availability of fixed PHP packages, at the time of this update. We will update this table as each source is confirmed:

PACKAGE SOURCE	AVAILABILITY
Linux distributions and LTS vendors	Received the patches in advance. Check your vendor for updated packages
Remi repository (RHEL-based, php:remi-8.2 to 8.5)	Not yet confirmed. The PHP project said the repository would not have updates on 21 October 2026
ppa:ondrej/php (Ubuntu)	Not yet confirmed
Docker (rconfig/rconfig on Docker Hub)	Not yet confirmed. The rConfig image is built on the official PHP image (php:8.4-apache-bookworm), so an updated rConfig image depends on that upstream image being updated first

After patching

If your rConfig server was reachable from the public internet, rotate all secrets and passwords on the server after you have patched.

Exploitation and public announcements

The PHP project's advisories describe both issues technically and confirm remote code execution against mod_php and PHP-FPM. CERT-EU does not report any exploitation of these vulnerabilities in its advisory.

CERT-EU's statement that the issues could affect all PHP versions from PHP 5 onwards comes from posts on social media and has not been confirmed. The PHP project provided source backports for PHP 7.4, 8.0 and 8.1 only.

DATE (IST)	EVENT
20 October 2026, 20:33:27	CERT-EU publishes Security Advisory 2026-018 (CVE-2026-109618, CVE-2026-109619).
21 October 2026	The PHP project releases PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 and publishes its security advisories GHSA-6wmf-4rv5-p3rp and GHSA-w8hw-w9fx-j79w.

Source

This advisory was prepared by rConfig from the public sources below. It will be revised as the PHP Foundation publishes details and as our assessment progresses.

1. CERT-EU Security Advisory 2026-018, Critical Vulnerabilities in PHP:
<https://cert.europa.eu/publications/security-advisories/2026-018/>
2. PHP Foundation announcement, 20 October 2026:
<https://www.php.net/archive/2026.php#2026-10-20-1>
3. PHP Foundation (X), release announcement:
<https://x.com/ThePHPF/status/2112828424486056183>
4. Remi repository (Bluesky), package availability:
<https://bsky.app/profile/remirepo.net/post/3mxyrvljtec27>
5. Ubuntu PHP PPA maintainer, issue tracking the fix:
<https://codeberg.org/oerdnj/deb.sury.org/issues/145>
6. PHP project security advisory GHSA-6wmf-4rv5-p3rp (CVE-2026-109619), RCE via stale global state: <https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
7. PHP project related security advisory GHSA-w8hw-w9fx-j79w:
<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>
8. PHP.net security advisory and release announcements, 21 October 2026:
<https://www.php.net/archive/2026.php>

rConfig security vulnerability policy

To report a vulnerability or ask about your deployment, email security@rconfig.com.

Revision history

VERSION	DESCRIPTION	SECTION	STATUS	DATE
0.9	Added Docker image availability.	Fixed software	Interim	21 October 2026, 15:47
0.8	Clarified that these are PHP vulnerabilities and that the fix is a PHP update.	Summary, Fixed software	Interim	21 October 2026, 15:25
0.7	Added the PHP project's release: fixed PHP versions, who is at risk, PHP 8.1 and older, package availability and mitigations.	Summary, Affected products, Workarounds, Fixed software	Interim	21 October 2026, 15:12
0.6	Added the PHP project's advisory: confirmed remote code execution and official mitigations.	Summary, Workarounds, Exploitation	Interim	21 October 2026, 15:08
0.4	Added the PHP versions each rConfig Pro and Core release runs on.	Affected products	Interim	21 October 2026, 11:55

VERSION	DESCRIPTION	SECTION	STATUS	DATE
0.3	Added the demo, CRM and portal hostnames that now redirect to www.rconfig.com .	Workarounds	Interim	21 October 2026, 10:00
0.1	Initial release.	All sections	Interim	21 October 2026, 09:32

Disclaimer

This advisory is based on information available at the time shown above, which may be incomplete or change. It is provided for information and does not create any warranty or commitment. Each change is recorded in the revision history.