

PHP2Shell Response Guide

Understand the threat. Replace vulnerable images. Verify the fix in production.

Two flaws in the PHP runtime

Disclosed October 21, 2026, PHP2Shell comprises **CVE-2026-109618** and **CVE-2026-109619**, both rated critical at CVSS 4.0 **9.2**. They can allow unauthenticated remote code execution in PHP itself. Web-facing PHP-FPM, Apache mod_php, php-cgi, FrankenPHP, and LiteSpeed installations need assessment. WordPress, Drupal, and Moodle can inherit the flaw through their embedded runtime; updating application plugins alone does not fix PHP. [PHP advisory](#)

1 CVE-2026-109618 - out-of-memory corruption. A crafted request can exhaust memory while PHP request data is incompletely initialized. Request cleanup can then consume invalid state. Apache mod_php has a demonstrated path before application code runs, which means application login controls may never get a chance to intervene. FPM behavior differs and must not be treated as immune. [OOM flaw](#)

2 CVE-2026-109619 - stale global state. A worker can retain references to memory belonging to a completed request. A later request to the same worker may access that freed memory before initialization clears the state. Successful exploitation depends on reachable producer and consumer operations, worker reuse, and suitable memory conditions. [Stale state flaw](#)

How exploitation can manifest

An attacker may submit malformed multipart requests or trigger an application error path to disturb memory handling. A successful exploit executes with the PHP process's permissions; it does not automatically confer host root access. AWS observed exploitation attempts as early as October 17, before public disclosure. Attempts do not prove that every targeted system was compromised. [OOM flaw](#), [Stale state flaw](#), [AWS findings](#)

Illustrative outcomes: On a WordPress site, execution could expose database credentials or allow content changes. On a Drupal portal or Moodle service, it could expose application-accessible records or create a web shell where writes are permitted. Failed attempts may instead cause worker crashes, restarts, or HTTP 5xx errors. These are plausible scenarios, not reports of specific victims.

Investigate: Look for unusual upload traffic, repeated memory errors, unexpected child processes, modified PHP files, and unexplained outbound connections. These signals are not specific proof of PHP2Shell. Preserve logs and assess possible credential exposure; deploying a patch does not remove an existing attacker foothold. [AWS findings](#)

How RapidFort fixes the exposure



Replace first. RapidFort provides patched curated equivalents for the image references on page 2. The patched runtime prevents unsafe cleanup after out-of-memory failure and clears request-owned state before freed memory is reused. Coverage includes supported PHP releases and the listed vendor-patched legacy entries. Upstream fixed baselines are **8.2.35**, **8.3.36**, **8.4.27**, and **8.5.12**; a vendor backport may retain an older version label. Use advisory and artifact evidence to verify coverage. [PHP advisory](#)



Rebuild and verify. Select the matching RapidFort image and variant, test extensions and application behavior, then redeploy every replica and restart long-running workers. Confirm running digests and patch evidence, including PHP copied from build stages or bundled in static binaries. RapidFort runtime profiling and hardening can then remove unused components; continuous monitoring helps track subsequent changes. [RapidFort platform](#)

Related PHP update: October 23 guidance addresses a separate session-upload-progress issue, CVE-2026-115560. Confirm its coverage independently; where required, keep `session.upload_progress.enabled=0` until the applicable fix is deployed. [PHP advisory](#)

Patched Image Coverage

39 RapidFort Images. These RapidFort Images are patched equivalents offered for this response. Obtain the RapidFort registry paths and immutable digests before deployment; the names below are not RapidFort pull commands.

drupal:10.6.19	php:8.4.27
drupal:11.3.19	php:8.4.27-apache
drupal:11.4.10	php:8.4.27-fpm
dunglas/frankenphp:1.10.1-builder-php8.4	php:8.4.27-zts
dunglas/frankenphp:1.10.1-php8.4	php:8.5.12
dunglas/frankenphp:1.10.1-static-builder-gnu	php:8.5.12-apache
dunglas/frankenphp:1.10.1-static-builder-musl	php:8.5.12-fpm
moodle:4.5.1	php:8.5.12-zts
moodle:4.5.15	renovate:43.255.2
moodle:5.1.8	renovatebot/base-image:13.71.6
moodle:5.2.4	serversideup/php:4.5.1-php-8.4-cli
moodle:5.3.0	serversideup/php:4.5.1-php-8.4-fpm-nginx
php:8.1.34	serversideup/php:4.5.1-php-8.4-frankenphp
php:8.1.34-apache	serversideup/php:4.5.1-php-8.5-cli
php:8.2.35	serversideup/php:4.5.1-php-8.5-fpm-nginx
php:8.2.35-apache	serversideup/php:4.5.1-php-8.5-frankenphp
php:8.3.36	serversideup/php:5.0.2-php-8.5-frankenphp
php:8.3.36-apache	wordpress:6.7.6-php8.4-apache
php:8.3.36-fpm	wordpress:7.1.3-php8.4-apache
php:8.3.36-zts	

Select the right variation

- 

FIPS and non-FIPS: RapidFort offers FIPS-capable and standard curated variants. FIPS concerns cryptographic modules and approved operating configurations; it does not fix PHP memory corruption. Choose a patched variant and verify its module validation, approved mode, and deployment requirements. FIPS coverage is not a claim that every container is itself a validated cryptographic module. Confirm availability for the selected tag, OS, and architecture. [FIPS variants](#)
- 

Apache, FPM, ZTS, and CLI: Apache integrates web serving; FPM uses FastCGI workers; ZTS denotes a thread-safe PHP build; CLI serves command-line workloads. Match the existing execution model and required extensions. Web-request exploit paths do not automatically apply to a CLI-only job, but copied or later-deployed PHP runtimes still need fixes. [PHP advisory](#), [PHP image variants](#)
- 

FrankenPHP and build variants: Retain the required embedded-server configuration. Builder images create downstream artifacts; replacing a builder requires rebuilding its outputs. GNU/glibc and musl variants target different C libraries. A static binary must contain patched PHP; updating OS packages around it is insufficient. Check Renovate and other tool images for PHP use and any artifacts they produce.
- 

Legacy coverage: PHP 8.1 is EOL upstream. For the two 8.1.34 references, retain RapidFort vendor-backport evidence and confirm ongoing support terms; an image listing does not restore upstream maintenance. [PHP advisory](#)

Get patched images: rapidfort.com/request-access | Match the tag, variant, architecture, and digest before rollout.

RapidFort is providing these images free of charge. Click [here](#) to obtain access.