

SECAUDIT 062 - Upstream PHP emergency infrastructure assurance

Audit ID	2026-10-21-062
Opened	2026-10-21
Closed	2026-10-21
Scope	Infrastructure that SnapSmack relies on: production web containers, SMACK CENTRAL, forums, skin registry/repository, directory and federation services.
Trigger	Upstream PHP runtime vulnerabilities CVE-2026-109618 and CVE-2026-109619 ("php2shell").
Status	CLOSED - affected PHP runtimes upgraded, services verified, Cloudflare managed protections confirmed, fleet integrity checked.
Product boundary	This was not a vulnerability or defect introduced by SnapSmack. It was emergency assurance and remediation of the upstream PHP runtime used by SnapSmack infrastructure.

Executive summary

On October 21, 2026, the PHP project released emergency security updates for two critical memory-state vulnerabilities affecting web-serving PHP installations. The flaws could permit unauthenticated remote code execution before application code had an opportunity to defend itself. No SnapSmack code change, plugin update or application rule could provide the complete fix; the PHP runtime had to be upgraded.

The SnapSmack infrastructure response upgraded every PHP-bearing production container, rebuilt the two Pixelfed application images on a fixed PHP release, validated the web and worker services, confirmed Cloudflare's managed php2shell protections, and completed a fleet integrity comparison. The database-only container did not run PHP and was not affected.

No evidence of exploitation or unexplained file modification was found. One integrity difference was the already-known, deliberate `fauxlaroid.fyi/assets/js/ss-engine-comms.js` hotfix; it was not treated as compromise.

What was affected

The vulnerabilities were in PHP itself, below SnapSmack's application boundary. They affected PHP web-serving configurations, including Apache module and PHP-FPM deployments. The PHP project's advisory rated immediate runtime updates as the required remediation and identified fixed releases 8.5.12, 8.4.27, 8.3.36 and 8.2.35.

Because the vulnerable processing could occur before application code ran, SnapSmack authentication, FAFO controls, request routing and CMS input validation were not substitutes for patching. Cloudflare WAF protections were useful defense in depth, not a replacement for a fixed runtime.

Remediation completed

Debian web and service containers

- CT101 through CT106 were upgraded to PHP 8.4.27.

- PHP syntax/runtime availability was checked after upgrade.
- Apache configuration validation passed and the services were active.
- Public application health checks returned expected successful responses.

Pixelfed containers

- CT107 and CT108 were rebuilt on PHP 8.5.12.
- The application, Horizon, scheduler and Redis services were verified healthy.
- CT107's public Pixelfed endpoint returned HTTP 200.
- CT108's internal host-routed endpoint returned HTTP 200. It had no public DNS record by design at the time of verification.

Database container

- CT110 ran MariaDB and did not run PHP. It was inspected for scope and correctly excluded from PHP remediation.

Cloudflare controls

Cloudflare's managed php2shell protections were confirmed active. Cloudflare stated that it deployed request-side managed rules and response/full-transaction detection, including protection for Free-plan zones, and would continue updating rules for mutated payloads.

No redundant custom rule blocking broad upload patterns was added. SnapSmack is a photography platform and requires legitimate image uploads; a coarse duplicate rule would raise false positives while adding little to the managed protections. Patched PHP remains the primary control.

Integrity and exposure review

- Thirty SnapSmack installations were checked against expected files.
- Twenty-nine were clean.
- The sole difference was the known deliberate fauxlaroid hotkey hotfix, already tracked as release provenance debt rather than unexplained compromise.
- No evidence of successful php2shell exploitation, unexpected web shells or unexplained application changes was found.
- PHP version disclosure was already disabled on public responses, which reduced passive fingerprinting but required host-side verification.

Findings and disposition

A. Upstream critical PHP runtime exposure - CLOSED

All PHP-bearing containers were moved to fixed upstream releases and service health was verified.

B. Edge protection as defense in depth - CLOSED

Cloudflare managed protections were confirmed active. The audit explicitly does not claim WAF coverage replaces patching.

C. Infrastructure inventory coverage - CLOSED FOR THIS EVENT

CT101 through CT108 and CT110 were explicitly reviewed. CT110's lack of PHP was verified rather than assumed. This closes the emergency scope, while the separate fleet-roster work continues to improve discovery of installations not

present in hand-maintained lists.

D. Evidence of compromise - NONE FOUND

The integrity sweep found no unexplained modification. This is evidence from the checks performed, not a claim that historical compromise is impossible.

Verification record

1. PHP versions: CT101-CT106 at 8.4.27; CT107-CT108 at 8.5.12.
2. Apache configuration valid and services active on the Debian web containers.
3. Pixelfed application, Horizon, scheduler and Redis healthy after rebuild.
4. CT107 public endpoint HTTP 200; CT108 internal routed endpoint HTTP 200.
5. CT110 confirmed outside PHP scope.
6. Cloudflare managed php2shell protection confirmed enabled.
7. Thirty-installation integrity pass completed: 29 clean, one known deliberate hotfix, zero unexplained differences.

Public references

- PHP project security notice and fixed releases: <https://www.php.net/>
- PHP 8.4.27 release announcement: https://www.php.net/releases/8_4_27.php
- Debian Security Advisory DSA-6574-1: <https://lists.debian.org/debian-security-announce/2026/msg00489.html>
- Cloudflare php2shell protections: <https://blog.cloudflare.com/php-vulnerabilities-waf-protection>

Closure statement

SECAUDIT 062 is closed. The vulnerable dependency was PHP, not SnapSmack. The purpose of this audit is to show that the infrastructure SnapSmack relies on - including its production sites, SMACK CENTRAL, forums, skin distribution services and related applications - was patched and checked promptly so users were not asked to rely on an unverified platform claim.