SERVICE ALERT

Prepared Nov 19, 2026, 11:27 AM PST

PHP Vulnerability

Status: Recovering / monitoring

Started Nov 19, 2026, 6:00 AM PST · Ongoing for 5 hours 28 minutes · PHP project's estimate: Upstream fix released 19 Nov 2026; distribution fixes not yet confirmed

PHP PROJECT REFERENCE NUMBERS

CVE-2026-129289 GHSA-qc49-hpvq-g2w6 CVE-2026-129474 CVE-2026-115560

Quote these to PHP project or to BIS support.

SUMMARY

PHP has released security updates for a critical flaw in PHP-FPM that could let an outside party run code on some websites. No exploitation has been reported. We are checking the Linux packages for the fixed version and will confirm what your server needs.

Affected: PHP-FPM, PHP 5.6 to 8.2.35, PHP 8.3 before 8.3.37, PHP 8.4 before 8.4.28, PHP 8.5 before 8.5.13

LATEST NEWS

PHP released fixes on 19 Nov 2026 for CVE-2026-129289 (critical PHP-FPM request smuggling) and other flaws. Upstream fixed versions exist; no exploitation is reported; Linux distribution packages are not yet confirmed.

PHP project says (Nov 19, 2026, 6:00 AM PST): “Security releases for all supported PHP versions, with CVE-2026-129289 rated critical; fixes in 8.5.13, 8.4.28, 8.3.37 and 8.2.36.”

Source: https://www.php.net/ChangeLog-8.php

WHAT YOU NEED TO DO

Tell us if your site runs PHP-FPM on a Linux server, so we can check its PHP version. Do not reopen persistent connections to PHP-FPM until the update is in place.

WHAT BIS COMPUTER SOLUTIONS, INC. IS DOING

We are checking the PHP and Linux distribution advisories for the fixed package on each server we manage. We will send the next update when a distribution publishes its fix.

IS THIS A HACK?

No — this is not a hack or cyberattack.

No exploitation has been reported as of 19 Nov 2026, but the flaw can be used to run code on some setups, so update now.

ROOT CAUSE

PHP-FPM can leave unread request-body bytes on a reused FastCGI connection, which are then parsed as a new request.

WHAT THE IT COMMUNITY IS SAYING

Admins and security people are posting today's PHP 8.5.13, 8.4.28, 8.3.37 and 8.2.36 security releases, mostly urging upgrades and naming the session-file flaw CVE-2026-126714 (phpAfterShell). Posters also share the interim fix of setting session.upload_progress.enabled to 0 and note that Redis- or database-backed sessions are not affected. No post in this batch reports a successful exploit or a breakage after patching, though one Drupal admin warns of a fatal error if upload_progress is On during the update.

From public posts by IT administrators; not confirmed by the vendor.

Questions? Contact BIS Computer Solutions, Inc.

Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com

LAST 2 UPDATES

Nov 19, 2026, 11:27 AM PST

BIS has had reports of another PHP vulnerability; the closest public match is the November 19, 2026 PHP security release, whose most serious flaw is CVE-2026-129289 (PHP-FPM request smuggling, rated critical), with fixed upstream versions 8.5.13, 8.4.28, 8.3.37 and 8.2.36, and no Linux distribution fix packages confirmed yet.

Nov 19, 2026, 11:22 AM PST

New PHP security release on 19 November 2026 fixes CVE-2026-129289 (critical PHP-FPM request smuggling) and other flaws, including CVE-2026-115560, in PHP 8.2.36, 8.3.37, 8.4.28 and 8.5.13.