SERVICE ALERT

Prepared Nov 26, 2026, 2:28 PM PST

PHPAfterShell

Status: Recovering / monitoring

Started Nov 19, 2026, 6:05 AM PST · PHP's estimate: Fixed upstream since Nov 19; distributions still rolling out; Debian testing, cPanel and NetApp not confirmed

WHAT HAPPENED

Several PHP flaws, including CVE-2026-126714 and CVE-2026-129289, are fixed in newer PHP versions, and Debian, Red Hat, Amazon Linux and Ubuntu have published updates. Servers running PHP need updating, and BIS is checking PHP versions on the servers we manage. We will send another update when Cisco confirms which of its products are affected.

DOES THIS AFFECT YOU?

Websites and apps that run PHP with the default file-based sessions may be affected. Sites where a front end reuses connections to PHP-FPM need checking too. If BIS manages your site, we are checking its PHP version for you.

WHAT BIS IS DOING

We are checking PHP versions on the servers we manage and will install the fixed builds. We are also watching Cisco's advisory and will send an update when Cisco confirms the affected products.

WHAT YOU NEED TO DO

If you run a website or application on PHP, ask us to check its version. Nothing else for now.

IS THIS A HACK?

No — this is not a hack or cyberattack.

LATEST UPDATES

Nov 26, 2026, 2:27 PM PST

New since the last run: Ubuntu's own CVE tracker now lists the fixed 26.04 and 26.10 packages, Cisco's Nov 24 advisory still lists no workarounds and is still checking products, and BIS has had reports of a workaround conflict and a Debian testing gap.

Nov 26, 2026, 2:22 PM PST

Fixed PHP releases for the November 19, 2026 flaws are out (8.2.36, 8.3.37, 8.4.28, 8.5.13, and 8.6.0), with a partial workaround only and no reported exploitation as of November 19.

Nov 26, 2026, 2:20 PM PST

New since the last check: Ubuntu 24.04 and 26.04 and cPanel fix listings, a NetApp interim advisory, Debian testing still unfixed, and a conflict over whether the upload_progress workaround helps; Cisco is unchanged.

WHAT THE IT COMMUNITY IS SAYING

The only allowed-site thread I found in this pass is the Hacker News discussion of the PHP 8.5.13 release, about six days old. Commenters say the fixed build needs session.upload_progress.enabled=1, which many admins had turned off as an earlier mitigation, and one unconfirmed comment says the fix is not complete yet. I found no Reddit posts, admin outage reports, 'fixed for me' confirmations, or Cisco discussion; the X posts I saw (including depthfirst's 'still vulnerable' claim) are outside the allowed sites and were not used.

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

For technical details (versions, patches and sources), ask BIS for the Technical brief.

Questions? Contact BIS Computer Solutions, Inc.

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