SERVICE ALERT

Prepared Nov 25, 2026, 9:48 AM PST

PHPAfterShell

Status: Recovering / monitoring

Started Nov 19, 2026, 6:05 AM PST · Cisco's estimate: Fixed upstream Nov 19; distribution packages still rolling out

WHAT HAPPENED

A flaw in PHP's default session handling (CVE-2026-126714) and a related PHP-FPM flaw (CVE-2026-129289) have fixed PHP versions available. 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 for Expressway 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 25, 2026, 8:05 AM PST

New since the last check: Amazon Linux and Debian fix reports, a Red Hat-family conflict, CVE-2026-129289 exploitation status as of Nov 20, and an unconfirmed Wordfence lab demonstration.

Nov 25, 2026, 4:03 AM PST

New: PHP's Nov 19 release date and advisory timing, a PHP2Shell link for CVE-2026-129481, unconfirmed distribution builds (Ubuntu, Rocky Linux), and no CISA KEV listing. Cisco's status is unchanged in this check.

Nov 25, 2026, 12:01 AM PST

New since the page was written: Cisco published its own phpAfterShell advisory (Nov 23, updated Nov 24), distribution builds are appearing, and no in-the-wild exploitation has been reported.

WHAT THE IT COMMUNITY IS SAYING

Posts from Nov 19 to 20 mostly announce the depthfirst disclosure of CVE-2026-126714 and the 8.2.36, 8.3.37, 8.4.28, 8.5.13 fixes, and urge upgrades. Some posts repeat a claim that the latest PHP releases are still vulnerable, while replies say PHP 8.4.28 and 8.5.13 fix it, and I found no posts reporting exploitation or Cisco or distro-specific fix confirmations.

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