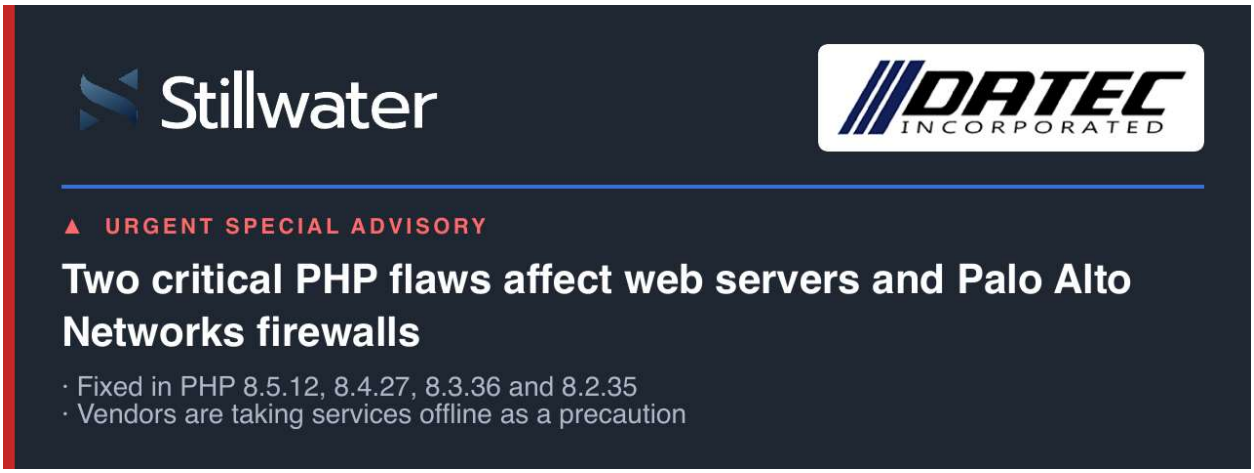


URGENT Special Advisory · October 21, 2026 · TLP:GREEN
In partnership with Datec

This is an urgent advisory. It is sent outside the weekly cycle because the timing matters.

Two Critical PHP Flaws Affect Web Servers and Palo Alto Networks Firewalls

PHP released fixes on October 21 for two flaws that "can allow unauthenticated remote code execution" (PHP). CVE-2026-109618 and CVE-2026-109619 are both rated critical at 9.2 on CVSS v4.0. Affected versions are PHP 8.5 before 8.5.12, 8.4 before 8.4.27, 8.3 before 8.3.36 and 8.2 before 8.2.35, plus 8.1 and older, which the PHP project no longer updates (CERT-EU). The flaws are in the PHP runtime, which comes from the server package, host or container image (The Hacker News). Updating WordPress or another application leaves them in place.

Palo Alto Networks says every version of PAN-OS and Panorama is affected, and it has no date for a fix. It rates the issue High, says no special configuration is needed to be affected, and knows of no exploitation against its products (Palo Alto Networks).

PHP rates Apache with mod_php the highest risk, "with a demonstrated exploit where an unauthenticated request can trigger the attack before any application code runs" (PHP). It also lists PHP-FPM, php-cgi, FrankenPHP and LiteSpeed as at risk. Red Hat rates CVE-2026-109618 Important. It says reliable exploitation needs precise heap manipulation and timing, and that remote code execution is difficult in practice on its standard PHP-FPM setup (Red Hat). On October 20, 59% of internet-facing hosts that report a PHP version ran PHP 8.1 or older, and some of those may carry a distribution backport (Mallory). PHP published only minimal source patches for 7.4, 8.0 and 8.1 (PHP).

Action: Update every internet-facing PHP server today, starting with Apache mod_php servers, which PHP rates highest risk, and FrankenPHP servers, which PHP's advisory says

are likely open to the same attack (GitHub advisory). Then restart PHP-FPM, Apache and any long-running PHP workers (PHP2Shell), and rebuild container images on a fixed PHP base. Confirm each fix from the package changelog, because distributions backport fixes under older version numbers (The Hacker News). Ubuntu 24.04's fixed package is 8.3.6-0ubuntu0.24.04.13 and Ubuntu 22.04's is 8.1.2-1ubuntu2.28 (Ubuntu). Debian shipped 8.4.27 for Debian 13 and 8.2.35 for Debian 12 (Debian). Red Hat had published no fixed packages as of 16:30 UTC (Red Hat). Treat Red Hat servers as unpatched until it does. Restrict access to PAN-OS and Panorama management interfaces until Palo Alto Networks ships fixed releases (Palo Alto Networks). Take any server you cannot patch off the internet until it is fixed (CERT-EU), or put it behind a VPN or an authenticating gateway (The Hacker News). PHP says its interim configuration settings "do not make an installation safe" (PHP).

Three Firms Report Attacks on PHP Servers

Hadrian reported exploitation "at scale" at 11:35 UTC, about two hours before PHP's fix, but has published no data and named no victim (Hadrian). Cloudflare saw attack traffic against its customers, with payloads reworked to try to get past its rules. It tells customers to patch even behind those rules (Cloudflare). watchTowr recorded exploitation on its honeypots (watchTowr). Huntress had seen none across its partner base at 14:00 UTC, Check Point said at 15:40 UTC that none had been reported, and the Dutch NCSC had seen none that morning (Huntress, Check Point, NOS). Neither flaw was in CISA's Known Exploited Vulnerabilities catalog at 16:30 UTC.

Action: After patching each server, check it for signs of compromise since October 20, when word of the flaws leaked (The Hacker News). Look for the web server launching command shells or download tools, unexpected files in the web root, and new scheduled tasks or accounts (Huntress). If you find any, isolate the server and preserve its web server and PHP logs. Remove stored credentials and cloud access roles from PHP servers that do not need them (The Hacker News).

Vendors Hold the Fix for PHP in Their Devices and Hosted Services

PHP is "embedded in appliances, network devices, management interfaces and other vendor products," and administrators may not be able to update it themselves (Dutch NCSC). Plesk says every PHP version it ships for Linux and Windows is affected (Dutch NCSC list). heise named routers and NAS units from QNAP, Synology, Zyxel, DrayTek, Netgear and others, and appliances from Citrix, Ivanti and F5, as products to check (heise). The Dutch NCSC lists products from QNAP, Synology, Citrix and F5 as under investigation (Dutch NCSC lists). Owners usually cannot update PHP on these devices themselves. Fixes come as maker updates, and stop at end of support. CISA's BOD 26-02 requires

federal civilian agencies to inventory and decommission internet-facing edge devices that no longer receive updates.

BambooHR took its US, Canadian and Irish service offline before PHP's fix was out, saying the outage interrupts essential work, including payroll (BambooHR status). In the Netherlands, government services including the DigiD citizen login went offline as precautions, as did Notubiz, a supplier's meeting system used by about 100 municipalities (NOS). We expect more providers to take services offline at short notice.

Action: Check each large vendor's status page or trust center first. Then ask your web host, managed service provider, control panel vendor and other key software and SaaS vendors in writing whether they run PHP and when they will patch it. Confirm a manual fallback for this week's payroll run and any other deadline that depends on a hosted service. List every device with a web management interface, including routers, firewalls, VPN gateways, NAS units and load balancers, and ask each maker whether it embeds PHP and when a fix will ship. Keep those management interfaces off the internet. Replace devices past end of support, and isolate them until you do.

Contact your Stillwater representative for help finding PHP across your systems and suppliers or reviewing a patched server.

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs. This advisory is distributed TLP:GREEN and may be shared within your organization and with sector peers.