

AI-found PHP flaws push governments and companies to take websites offline

Source copy kept by wheresthe.ai for the story "AI-found PHP flaws push governments and companies to take websites offline" (<https://wheresthe.ai/d/intl-ai-found-php-flaws-take-websites-offline-2026-10/>).

Source: <https://www.thehindu.com/sci-tech/technology/websites-go-dark-as-ai-exposes-critical-security-flaws/article71609942.ece>

Text saved 23 Oct 2026 (the page as published).

SHA-256 of the saved text: f9e00b8a4889aa52037d8768f7ca84b61f15f3a36d147956ea9cb2ba093d09b6

Websites go dark as AI exposes critical security flaws - The Hindu

You are logged in Loading... LOGOUT You don't have any Active Subscription. Subscribe now Subscribed with another email? Logout and Login with that one.

Your active subscription(s)

Account subscription benefits alongside Premium Stories, Editorials, Opinions and more. Unlock these with Subscription

Products you've access to

Additional Subscription Benefits

eBooks Webinars Newsletters Games Monthly Digest Account Settings Go to My Account Bookmarks Manage Subscriptions

Need help with your subscription? customersupport@thehindu.co.in 1800 102 1878

Websites go dark as AI exposes critical security flaws

PHP sits underneath popular web design platforms, so the weaknesses potentially affect a vast range of websites
Published - October 22, 2026 09:02 am IST

AFP

READ LATER SEE ALL

Remove

Only sites that run PHP on their own servers are exposed [File] | Photo Credit: REUTERS

Government agencies and companies around the world shut down websites Wednesday after two critical flaws came to light involving PHP, a programming language that is the basis for a large share of the internet. PHP sits underneath popular web design platforms, so the weaknesses potentially affect a vast range of websites, from online stores and news outlets to government services. Wiz, one of the security firms that found the flaws, estimated that PHP runs about 70 percent of the world's websites and said they rank "among the most severe vulnerabilities discovered in PHP, and arguably in software history." The US National Security Agency told organisations to patch immediately or pull vulnerable systems offline. Only sites that run PHP on their own servers are exposed. Many large platforms are built on other programming languages or use operators that could install the fix quickly and were able to stay online.

After Musk 'punishes' Ukraine, how exposed is India to foreign tech?

The flaws "often provide a direct path to the server's file system or database," the NSA said in a statement on X. Attackers could use them to take over web servers without needing a password. Volker Dusch, a security engineer at the PHP Foundation, told the Wall Street Journal it was the most serious problem PHP had faced in more than a decade, comparing it to Heartbleed, a 2014 flaw that set off a worldwide rush to patch. The discovery came amid a surge in software security disclosures driven by increasingly powerful AI models, with the number of vulnerabilities found in 2026 on track to roughly double last year's record total. PHP programmers released a fix on Wednesday. "If you run PHP, it is imperative that you update now," the PHP Foundation, which funds developers working on the language, said in a blog post. Security firm Calif found the flaws in August using

OpenAI's GPT-5.6 Sol model, as part of an OpenAI-funded audit of PHP's code. Wiz, which is owned by Google, said it found them independently weeks later with help from AI models including Google's Gemini 4 Argon and GPT-5.6 Sol. OpenAI said on X that it considered the flaws "one of the most impactful vulnerabilities in recent memory," adding that the discovery "marks a new phase, where AI can find security bugs with internet-scale impact." Ethan Mollick, a professor at the University of Pennsylvania's Wharton School who studies AI, said companies he talks to are struggling to keep up with the pace of patches needed to guard against AI-driven cyberattacks. "Now consumers are going to have the same experience of getting everything updated often and fast," he wrote on X. The flaws had been reported privately to PHP's developers and kept confidential while a fix was prepared. Details leaked online Tuesday, a day before the planned release of the fix, prompting the rush to take sites offline before hackers could exploit them. In France, local government websites, including one for the Paris police, were made inaccessible at the request of the French National Cybersecurity Agency, the interior ministry said. In the Netherlands, the national digital identity service DigiD, the website of the House of Representatives and the site of the national cybersecurity center went offline as a precaution, according to Dutch public broadcaster NOS.

Eight web security keys of eMudhra firm used by Govt. and PSUs leaked

In Australia, the Australian Signals Directorate said its own cyber.gov.au site was among government websites affected by the flaws, according to Australian public broadcaster ABC. The Wikimedia Foundation, which runs Wikipedia, warned users they could see outages on its sites while it addressed the flaws, and said it had deliberately taken many of its supporting services offline until they could be safely patched. Several Pokemon apps, including Pokemon HOME, Pokemon Champions and Pokemon Sleep, also went offline Wednesday for emergency maintenance, with Pokemon Sleep citing security measures, according to gaming news site Kotaku. The operator of the hit Japanese game Umamusume said it was carrying out maintenance to fix a PHP vulnerability found in its servers.

Published - October 22, 2026 09:02 am IST

[Read Comments](#) [Copy link](#)

[Email](#)

[Facebook](#)

[Twitter](#)

[Telegram](#)

[LinkedIn](#)

[WhatsApp](#)

[Reddit](#)

[READ LATER](#) [SEE ALL](#)

[Remove](#)

[Related stories](#)

[Cyber agency warns websites may go dark as PHP prepares critical fix](#)

[Data breach: SBI admits exposure of its customer data on the Dark Web](#)

[Unknown vulnerabilities: on the cybersecurity advisory by CERT-In](#)

[Why Big Tech is giving away open-weight AI models, and what it wants in return | Explained](#)

[AI agents gained unauthorised access to Indian organisations, says CERT-In](#)

[Related Topics](#)

[technology \(general\)](#)

0 / 0

Middle Sticky container -->

Sign in to unlock member-only benefits! Access 10 free stories every month Save stories to read later Access to comment on every story Sign-up/manage your newsletter subscriptions with a single click Get notified by email for early access to discounts & offers on our products

× Looks like you are already logged in from more than 5 devices! To continue logging in, remove at least one device from the below list

Log out di.payload), 'all')">Log Out from all devices [Terms & conditions](#) | [Institutional Subscriber](#)

Comments Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments. We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.