World Socialist Web Site **wsws.org**

Discovery of security vulnerabilities in PHP programming language triggers global internet shutdowns

Kevin Reed
22 October 2026

A pair of flaws in PHP, a programming language embedded in a vast share of the world’s web infrastructure, forced governments, corporations and public institutions to take websites and online services offline on Wednesday. The crisis demonstrated how artificial intelligence (AI) can rapidly expose defects buried for years in essential digital systems and how the same technology can compress the time needed to defend them.

PHP originally stood for “Personal Home Page,” though the name is now recursively defined as “PHP: Hypertext Preprocessor.” In plain language, it is software that runs behind the scenes on web servers: when a person clicks a link, signs into an account or fills out a government form, PHP can process the request, retrieve data and generate the page sent back to the browser.

It is used by many custom-built websites and applications using platforms like WordPress and Drupal, meaning that an error in PHP is not confined to one company or one web service. The *Wall Street Journal*, which first reported the issue, said PHP “powers as much as 70 percent of the world’s websites” and that the newly disclosed flaw “could be leveraged by hackers to take control of any system running its software.” The *Journal* also reported that hackers could exploit the weakness “in many ways, some requiring just a few seconds,” to run unauthorized software on an unpatched server.

The vulnerabilities, collectively labeled PHP2Shell, are tracked as CVE-2026-109618 and CVE-2026-109619. Both received a critical industry severity score of 9.2 out of 10, and both can potentially allow an attacker with no password, account or direct access to a machine to run commands remotely on a vulnerable server.

One flaw concerns what occurs when PHP exhausts the memory allocated to it while assembling data from an incoming web request. Put simply, PHP can be interrupted halfway through preparing its internal response, then later mishandle the incomplete remnants as though they were valid. The second is a “use-after-free” defect: PHP can retain a reference to information after the computer has released the memory where it was stored, allowing a later request to exploit that stale reference.

For an ordinary user, the practical danger is straightforward. A malicious visitor might send specially constructed requests to a website, seize control of the limited account used to run its web service, steal information visible to that service, install malicious software, alter material or shut the site down. The Singapore Cyber Security Agency warned that successful exploitation could enable “unauthenticated remote code execution”—the technical term for an outsider causing a computer to run code of the attacker’s choosing.

The flaws affected PHP releases from version 5.4 through 8.5.11. Systems based on PHP 8.1 or earlier were in a particularly precarious position: those releases had already reached end-of-life and were not receiving new fixes from the PHP project. These include systems running software that is up to 14 years and seven months old.

The crisis exposed the degree to which basic public services are dependent upon shared, frequently outdated software components. Rather than risk allowing attacks into public-facing systems, agencies

© World Socialist Web Site

across Europe took services down while emergency updates were installed and systems were checked.

Examples of the impact of the vulnerability included:

- Finland, where state IT provider Valtori took government public web-network services offline Wednesday as a "precautionary measure."
- France, where the Interior Ministry temporarily shut websites for prefectures—the local administrative offices through which residents access numerous state services—while awaiting a security fix.
- The Netherlands, where the National Cyber Security Centre took its own public website offline.

Media reports indicated that the crisis did not consist of one centralized failure that could be timed from beginning to end, but a series of emergency withdrawals of public and commercial services as separate organizations raced to assess exposure, install fixes and restore operations.

The PHP project released emergency versions of its software at about 9:30 a.m. Eastern Time on Wednesday. The project urged users to update immediately. Patching was not automatic, however, and required action by each organization, hosting provider or systems administrator.

AI was central to both the discovery of the vulnerabilities and fears about their weaponization. Security firm Calif found the defects during an OpenAI-funded examination of PHP using OpenAI's GPT-5.6 Sol model, while Google-owned Wiz independently reported finding the flaws using AI systems including Google's Gemini 4 Argon and GPT-5.6 Sol.

According to Wiz, AI helped uncover weaknesses that had "remained hidden in the PHP codebase for more than a decade," describing the episode as an "AI inflection point." The implication is not merely that a machine helped find a bug, but that AI-assisted analysis can search huge and intricate bodies of source code faster than traditional manual review—and can do so across critical infrastructure software maintained with limited resources.

The danger was that the same systems could help attackers analyze released patches, infer the underlying bug and generate working attack code at exceptional speed. OpenAI itself warned that AI can identify "security flaws with internet-scale impact," while also enabling attackers to "rapidly develop offensive tools and exploits."

Calif chief executive Thai Duong put the threat starkly in comments reported by the *Wall Street Journal*: "Some dude on Twitter could take the patches and run AI against it and post some exploit script. All hell will break loose."

This did not mean that every online attacker instantly possessed a fully functional automated weapon. The defects were described as having high attack complexity, even though they required no authenticated account or user interaction. But AI fundamentally changed the tempo: the traditional interval between publication of a software patch and the emergence of public exploit code could be reduced from days or weeks to hours or less.

The PHP crisis follows a series of internet-scale emergencies in which a defect in a broadly shared component has disrupted millions of people or placed vast quantities of data at risk. Such events repeatedly expose the contradiction between the social character of digital infrastructure and its subordination to private ownership, competitive advantage and cost-cutting.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact