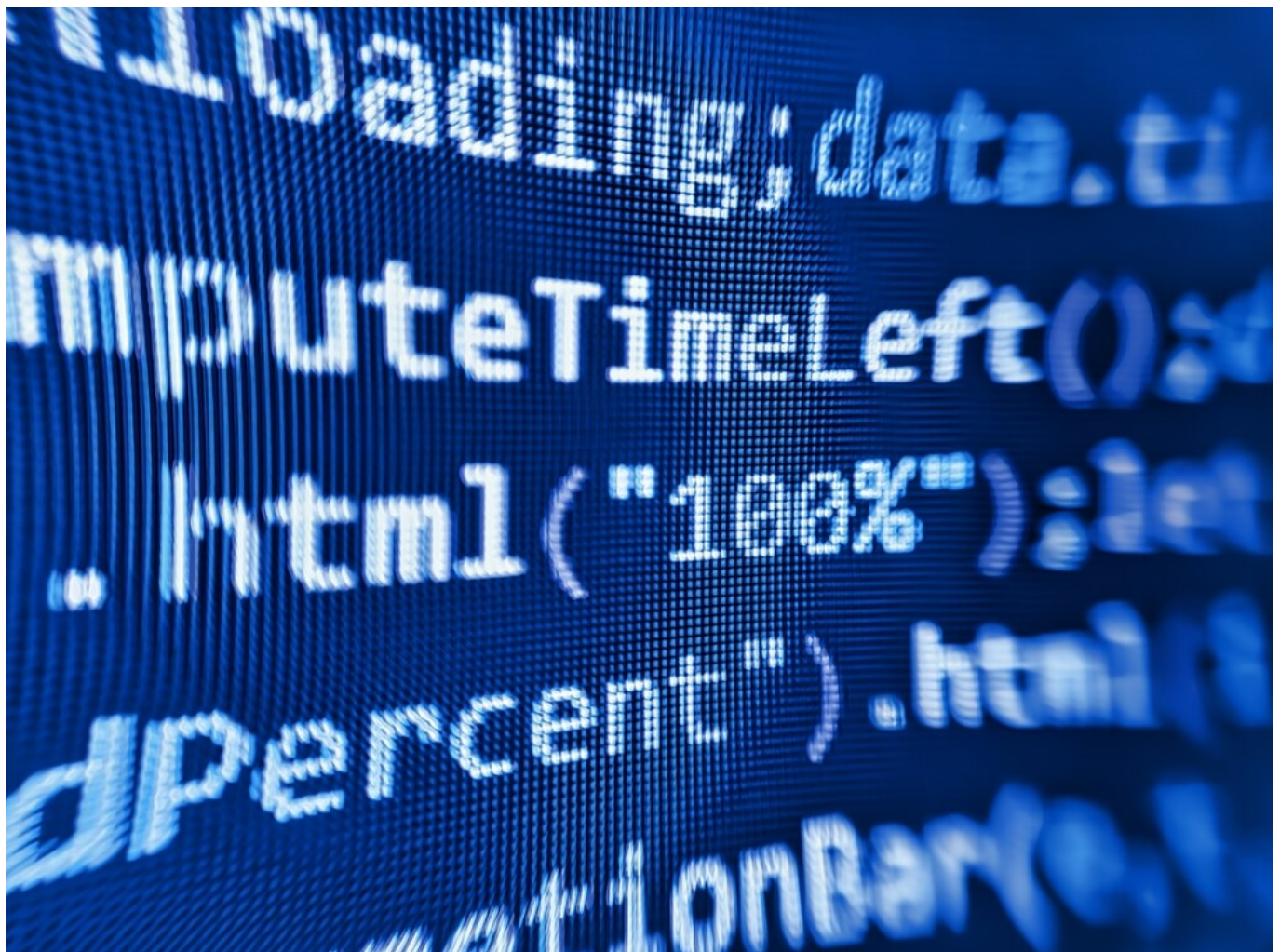




By: Tomorrow's Affairs Staff

European public services depend on software maintained by too few experts



On 21 October, the Dutch government temporarily shut down the portals [Overheid.nl](#) and [MijnOverheid](#), through which citizens access state information and their data, as well as DigiD, the system used to register for electronic public services.

The Port of Rotterdam, hospitals and the websites of the largest political parties were among those [affected](#).

Germany's federal information service, ITZBund, suspended part of its government websites, France's Ministry of the Interior temporarily shut down prefecture websites, and Finland's state information centre, Valtori, shut down the government's public internet services.

Preventive shutdowns also took place in Belgium, and in the Czech Republic the government website was unavailable for about two hours.

The [European Patent Office](#) suspended access to certain electronic services and began to restore them once security updates had been installed.

The cause was two critical flaws in PHP, the programming language that processes requests from website visitors on servers.

According to [W3Techs](#), PHP is used by 69.3 per cent of sites for which the server-side programming language is known.

Popular systems such as WordPress, Drupal and Joomla run on it, so it underpins a large number of government, school and hospital websites.

The flaws that were discovered allowed attackers, under certain conditions, to issue commands to the server without a username or password.

Most of the European shutdowns were preventive, as institutions were waiting for the publication of fixes.

An unavailable portal does not mean that data

has been stolen or that an attack has succeeded.

The 2012 flaw remained unresolved even after the security check

According to security researchers, the oldest piece of compromised code comes from a version of PHP released in 2012.

One of the two key issues was identified while reviewing the results of a 2024 security audit.

The audit was funded by the Sovereign Tech Agency, Germany's state agency for supporting open-source software.

[PHP is free to use, but maintaining it securely requires ongoing funding and people with many years of experience](#)

While fixing one of the reported weaknesses, a developer on the PHP core development team noticed a problem in the handling of computer memory.

At that time, no one had yet demonstrated how an attacker could use it to take over a server.

Any solution considered could disrupt existing applications, slow them down, or introduce new security problems.

The team revisited the same questions for months, and decisions were delayed because only a small number of developers knew that part of PHP in detail.

On 21 October, the foundation admitted that the delay was due to a slow decision-making process and a shortage of experts.

PHP is free to use, but maintaining it securely requires ongoing funding and people with many years of experience.

Fixes remained the work of a few people

The breakthrough came when researchers used an artificial intelligence model to demonstrate how a long-known weakness could be exploited to take over a server.

In June, OpenAI launched the **Patch the Planet** programme with the company Trail of Bits, in which artificial intelligence searches for vulnerabilities in open-source software.

As part of that programme, the American security research company **Calif** chose PHP as the subject of verification and, using OpenAI's GPT-5.6 Sol model, found a serious flaw.

Independently of Calif, Wiz discovered related vulnerabilities on 19 August, using Google's Gemini 4 Argon model, OpenAI's GPT-5.6 Sol and its own Wiz Atlas system. Both research teams reported their findings to the PHP developers in August.

According to Wiz researchers, the models helped them chain multiple bugs into a single attack process, adapt it to different PHP versions and server settings, and quickly fix anything that failed during attempts.

Wiz claims that one researcher did in a week what would previously have taken the team months.

A small group of developers paid by the foundation, supported by volunteers, carry out the fixes

By that assessment, turning a known weakness into an exploitable attack now requires much less specialised work.

These findings made fixing the problem a top priority for the PHP team. According to the foundation, research supported by **artificial intelligence** has greatly increased the number of reports that someone has to review.

Since 1 July, 15 new vulnerabilities have been

published with an official flag, and more than 100 reports that turned out to be incorrect, duplicates or unverifiable have been processed.

The foundation itself uses artificial intelligence to check reports and group those with the same cause, but people make the decision on each fix.

A small group of developers paid by the foundation, supported by volunteers, carry out the fixes.

They must review each change to ensure it does not cause problems in the large number of applications that use PHP.

Attack attempts began before the fixes were released

On 17 October, **Amazon** recorded an attempt to exploit the vulnerability on one of its servers set up as bait for attackers.

According to Amazon, this shows that a potential attacker had enough information to launch an attack four days before the public release.

It is not known how they obtained this information, or whether the attempt would have succeeded against the real system.

That attempt preceded both the leak of vulnerability tags and the premature release of a fix pack, so later coordination errors do not explain it. There is no evidence that artificial intelligence was used.

On 21 October, Amazon recorded additional attempts, including some that preceded the official release of the fixes.

Institutions that have installed the new version and reactivated the site have one more task.

Their experts must check records of previous access to the server, unusual file changes and other warnings that might indicate that

someone has already exploited the weakness.

The patch prevents new attacks through the known vulnerability, but does not repair damage if an intrusion has already succeeded

The patch prevents new attacks through the known vulnerability, but does not repair damage if an intrusion has already succeeded.

Such verification takes time, especially in organisations that do not have their own cyber-incident monitoring team.

The PHP team had planned to release the fixes on 22 October, but on 20 October, tags for two vulnerabilities began circulating on the internet, containing incorrect information about their severity and release dates.

The publication of the corrections was therefore brought forward to 21 October.

Calif also mistakenly released a video demonstrating the attack, which quickly went viral.

Chainguard, which distributes software packages, released the fix packs on 21 October, more than six hours ahead of schedule.

The PHP Foundation considered this a breach of contract, because by comparing the old and new versions it was possible to identify a vulnerable part of the code while most users were still waiting for the official release.

The early announcement further reduced the time available to prepare protection.

The most expensive update awaits users of older versions

Out-of-the-box **security fixes** have been released for supported versions of PHP 8.2 to 8.5. For versions 7.4 to 8.1, only source code changes are available, which must be installed separately or obtained from the operating

system supplier. For releases 5.4 to 7.3, the PHP team has not issued a fix.

This is an additional problem for institutions whose portals depend on software built many years ago, because switching to a new version can require costly changes to the entire application.

Approximately 35 per cent of sites using PHP with a recognised version are still running version 7 or older

According to W3Techs, approximately 35 per cent of sites using PHP with a recognised version are still running version 7 or older.

This does not mean that all of them are unprotected, as some manufacturers and distributors provide their own security patches.

It does show, however, how widespread software is for which a simple upgrade is often not available.

In the case of **public institutions**, the matter is further complicated by contracts with external suppliers.

They maintain the application, but its core components come from other projects.

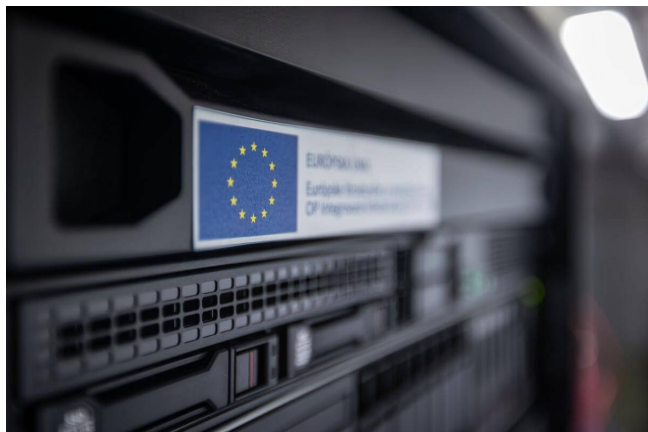
In a hospital or municipality, switching to a newer version can therefore mean checking electronic forms, data exchange and other functions that have been used for years without significant changes.

Who pays the developers that state services depend on

The European Commission, the EU Agency for Cybersecurity (ENISA), CERT-EU, Europol and the network of national cybersecurity teams issued a joint warning on 21 October.

They urged organisations to identify which of

their services use PHP, install fixes and, where this is not immediately possible, temporarily disconnect affected systems from the internet.



The EU regulations govern legal responsibility and emergency response, but they do not provide funding for the people who maintain PHP

Under **Europe's Cyber Resilience Act**, certain digital product manufacturers have been required, since 11 September, to report vulnerabilities that are being actively exploited.

The main security requirements apply from December 2027, when special obligations also begin for organisations designated by law as stewards of open-source software.

These regulations govern legal responsibility and emergency response, but they do not provide funding for the people who maintain PHP.

The PHP Foundation employed 11 full-time or part-time developers at the end of 2025 to develop and maintain the language as a whole.

That year, it received about \$645,000 in donations after fees from 536 companies and individuals, and spent \$784,000.

It covered the difference of about \$139,000 because, according to its own report, it has healthy reserves.

Germany's Sovereign Tech Agency invested €205,000 in PHP during 2023 and 2024, including a security audit, and approved another €223,000 for 2025 and 2026, also including security work.

Public support, therefore, exists and continues. However, it still has not provided enough experts for the most sensitive security roles, which the foundation itself is now warning about.

Subsequent attacks will target the hardest-to-update servers

Government institutions that were able to install the patches quickly are bringing their portals back online.

In the coming weeks, attackers will increasingly look for servers running outdated versions of PHP, especially where replacing the core programme also requires changes to other systems.

The most exposed institutions are those that have been using the same applications for years and do not have a reliable overview of the software on their servers.

Public purchasers will increasingly ask suppliers for a precise list of the programmes they maintain and for shorter deadlines for deploying emergency security fixes

Public purchasers will increasingly ask suppliers for a precise list of the programmes they maintain and for shorter deadlines for deploying emergency security fixes.

Such contracts can speed up the response, but replacing an outdated system takes much longer.

OpenAI expects the number of similar findings to rise sharply in the coming months, along with the workload for the small teams that maintain widely used software.

The PHP Foundation has hired new experts and is changing how it makes decisions.

Additional donations can quickly increase its budget, but the expertise needed to fix the most sensitive parts of a programming language is developed over many years.

At the next serious warning, facilities with up-to-date systems will shut down their portals again and wait for several developers to complete the fixes.

Institutions that depend on unsupported versions and applications that are difficult to modify will remain exposed, as a security update may require a full system rebuild they have been putting off for years.