

ISS GLOBAL / INCIDENT INVESTIGATION



PHP security alert: widespread website shutdowns

Precautionary service suspensions reported on 21 October 2026

REPORTING / REVIEW WINDOW

ISSUE DATE

21 October 2026, 00:00–23:59 Europe/London. Advance warning of 2026-10-22
20 October included as context; research retrieved 22 October.

Official notices establish that multiple operators withdrew online services while responding to critical PHP vulnerabilities. The evidence supports a widespread precautionary disruption; it does not establish that every unavailable website was compromised.

Principal judgement

A common software dependency created an urgent repair problem across otherwise separate organisations. Operator decisions to isolate services explain the documented cases. An outage, a vulnerable system and a confirmed intrusion must be recorded separately. ^[4] ^[6] ^[7]

Inside this report

Reconstruction; technical cause; warning and patch chronology; confirmed service impacts; evidence and attribution audit; restoration assurance; unresolved questions and ten linked primary sources.

Issue prepared on 22 October 2026. Public-source assessment; no private system logs or forensic exhibits examined.

01 / RECONSTRUCTION

A security alert became a service disruption

The initiating event

The PHP project announced an emergency security release on 20 October, scheduled for 14:00 UTC the following day. Its 21 October advisory identifies two critical vulnerabilities capable of unauthenticated remote code execution. This is a shared software exposure affecting systems that use PHP to serve web requests. ^[1]

The operator response

The Dutch government confirms that Overheid.nl, MijnOverheid.nl and DigiD were among sites taken offline as a precaution on 21 October. It also says many government websites, including Rijksoverheid.nl, did not use PHP and were unaffected by this vulnerability. ^[4]

ASIMUT states that it suspended access while waiting to apply and verify security updates. Georgetown University says it was taking affected servers offline immediately to install updates, warning that university websites and services could experience temporary downtime. These are separate operators describing their own actions. ^{[6] [7]}

ISS Global assessment

The strongest supported explanation for these examples is protective withdrawal of services while an urgent repair was prepared and deployed. Users experienced unavailability, but that symptom alone cannot identify a cyberattack. A shared vulnerability explains why independent organisations could make similar decisions within the same reporting period.

The reviewed evidence establishes a multi-organisation disruption. It does not establish a single internet-wide failure, a complete list of affected sites or one simultaneous start and end time. Those stronger claims would require a defined measurement set and timestamped service records.

02 / TECHNICAL CAUSE

What the vulnerabilities mean

IDENTIFIER	VENDOR EXPLANATION	OPERATIONAL SIGNIFICANCE
CVE-2026-109618	Out-of-memory handling can leave request data incompletely initialised.	Subsequent processing can lead to memory corruption and remote code execution. [1]
CVE-2026-109619	Internal request state can remain after its backing memory is freed.	A later request can encounter stale state, enabling remote code execution. [1]

Vendor source: [1]

PHP lists fixed releases as 8.5.12, 8.4.27, 8.3.36 and 8.2.35. It identifies all web-request-serving installations as at risk, with Apache mod_php the highest-risk configuration in its assessment. Deployment details matter; exposure does not mean every configuration is equally exploitable. [1]

Why a website login was not a sufficient boundary

The UK NCSC warns that the issue can permit unauthenticated execution under particular conditions. Its advice is to identify PHP across infrastructure, prioritise public-facing systems, apply vendor updates and consider taking systems offline when updates and temporary controls cannot be applied in time. [2]

Scope beyond public pages

The Swiss NCSC includes internal applications, administration interfaces, hosting platforms, containers and appliances in the discovery task. It warns that a provider may backport fixes without changing the main version number, making the exact package and supplier security record important. [8]

ISS Global interpretation

A page can look static while its supporting service uses a vulnerable component. Equally, a website built without PHP is not shown to be affected merely because PHP is widely used elsewhere. The correct unit of assessment is the deployed application and its actual dependencies.

Warning, withdrawal and patching

DATE / TIME	DOCUMENTED DEVELOPMENT	INTERPRETATION
20 October	PHP gives advance notice of a critical release. [1]	Preparation window; no universal outage start.
21 October, before release	ASIMUT announces suspension pending updates. [6]	Direct statement of preventive action.
21 October, 13:30 UTC / 14:30 BST	CERT-EU reports that fixes were released at 13:30 UTC. [3]	Attributed release time; earlier than the announced schedule.
21 October, 15:13 CEST / 14:13 BST	Dutch government notice names suspended services. [4]	Publication time, not each service's shutdown time.
21 October, 15:50 CEST / 14:50 BST	Dutch NCSC community update says patches are available. [5]	Communication timestamp, not a competing release timestamp.
21 October, 20:40 CEST / 19:40 BST	Dutch NCSC update says its main website is accessible again. [5]	Evidence of that site's return; other services not implied.

Linked chronology sources: [1] [3] [4] [5] [6]

Timing audit

The planned release was 14:00 UTC, equivalent to 15:00 BST and 16:00 CEST. CERT-EU gives an earlier actual time. ASIMUT's estimate was restoration approximately 45 minutes after the expected release, conditional on successful deployment and verification; it is not used as an observed recovery time. [3] [6]

The Dutch government page retains pre-release wording alongside an untimed update that patches are available. These evolving notices should be read as a sequence of communications, rather than evidence that the patch was unavailable at every timestamp shown. [4]

No complete per-service downtime interval can be calculated from these notices. Subtracting a publication time from a forecast would create an unsupported duration.

Which services were affected?

ORGANISATION / SERVICE	WHAT THE ORIGINAL SOURCE SUPPORTS	WHAT REMAINS UNKNOWN
Dutch government services	Precautionary suspension of named public portals. [4]	Exact duration, user totals, transaction backlog.
NCSC Netherlands	Its own main website temporarily offline; community used for updates, later return noted. [5]	Exact withdrawal time and full restoration test results.
ASIMUT	Access temporarily suspended pending updates and verification. [6]	Observed recovery time and number of users affected.
Georgetown University	Affected servers taken offline for patching; possible website and service downtime. [7]	Specific service list and completed restoration time.

Direct statements: [4] [5] [6] [7]

Consequences: ISS Global assessment

Loss of access to public portals can prevent a user from completing a task even when data remains intact. Scheduling and education systems create different continuity demands, including alternative access, deadline handling and communication with users. These are plausible operational consequences; the sources do not quantify lost transactions or missed activities.

Limits on scale

This is a documented case set, not a census. It provides evidence across public administration, commercial software and higher education. The number of PHP-dependent websites is not the number taken offline, and neither figure is a count of compromised systems.

Authority alert versus outage record

NHS England published a high-severity alert and judged future exploitation highly likely. That establishes a health-sector warning, not an NHS outage. Drupal’s notice assigns responsibility for platform maintenance to owners and hosts; it does not establish that Drupal.org was unavailable. [9] [10]

No loss estimate, confirmed data theft, casualties or named malicious operator is established for this selected case set.

05 / EVIDENCE AND ATTRIBUTION

Exposure, attack and compromise are distinct

QUESTION	EVIDENCE AT REPORTING CUTOFF	CONFIDENCE / QUALIFICATION
Were serious vulnerabilities real?	Maintainer advisory and fixed releases. [1]	High: original vendor record.
Were services withdrawn deliberately?	Direct operator and government statements. [4,6,7]	High for the statements; no independent uptime dataset reviewed.
Was exploitation technically possible?	NHS alert reports successful researcher demonstrations. [10]	Established reporting; not a real-world victim count.
Was malicious exploitation confirmed?	Dutch initial notice reports no detected active abuse; CERT-EU warns of increased likelihood. [3,5]	Different times and evidential categories; no victim proof here.
Who caused the disruption?	Named operators describe precautionary decisions.	No supported malicious-actor attribution for these shutdowns.

Sources for audit: [1] [3] [4] [5] [6] [7] [10]

The apparent contradiction

A statement that an authority has not detected active exploitation is bounded by its visibility and time. A forecast that exploitation is likely is a risk assessment. Neither statement proves universal safety or confirms that a particular service was breached. The report retains both with their status intact.

Source independence

PHP is the upstream source for the vulnerability and repair. Security authorities largely interpret that same technical finding; their repetition is not independent discovery of ten separate flaws. Operator notices do independently establish different decisions to withdraw services.

What was not examined

No affected organisation's server logs, incident-response images, provider change records or independent availability measurements were available. No authenticated incident imagery was required to establish a precautionary software shutdown. A geographic map would imply a physical footprint that these records do not measure, so none is used.

What a credible restoration should establish

Published guidance

Drupal directs owners who manage PHP themselves to update it, and those using managed hosting to follow their host's communications. Its notice stresses that a PHP release containing the fix is the complete mitigation. Responsibility for third-party platform maintenance remains with site owners and their suppliers. ^[9]

The Swiss NCSC recommends restarting affected services and long-running processes after updates, checking that the running application uses a fixed package, and inspecting for anomalies. It explicitly notes that an update cannot undo a compromise that has already occurred. Temporary controls reduce particular paths and do not replace patching. ^[8]

Suggested assurance record: ISS Global assessment

1. **Scope:** identify the service, owner, PHP dependency, deployment and supplier, including externally managed components.
2. **Containment:** record when access was restricted, the reason, approved exceptions and the customer-facing alternative.
3. **Repair:** retain the supplier advisory, fixed package identifier and deployment record for each instance.
4. **Runtime verification:** confirm active services use the repaired build; do not rely solely on an installed package list.
5. **Recovery:** check essential user journeys and supporting services before recording restoration.
6. **Security review:** preserve evidence of suspicious activity and track investigation separately from availability recovery.

Reporting to leadership

An assurance statement should say which services were checked and what remains outstanding. "Website back online" answers an availability question; it does not establish that every dependency was repaired or that an earlier compromise has been excluded.

This investigation does not assess ISS Global's own website exposure. That would require a separate review of its hosting and deployed dependencies; the current report concerns the wider public incident.

Assessment at the close of 21 October

Principal finding

ISS Global assesses the documented shutdowns as a precautionary availability impact arising from a serious shared software vulnerability. Independent operator statements support this explanation. The record does not support describing all affected services as hacked, nor attributing the incident to a common malicious actor.

Residual risk

NHS England's forecast of likely exploitation underlines the need for rapid repair, but a severity score is not a probability of compromise for a particular installation. Exposure must be assessed against deployment facts, and a security conclusion must be supported by local evidence. ^[10]

Priority unresolved questions

- Which additional operators actually withdrew services, rather than merely publishing an advisory?
- What were the verified start and recovery times for each service?
- Which repaired package was running on each affected instance at reopening?
- Was any malicious activity detected, and was it linked to either vulnerability?
- What user impact remained after restoration, including queued work and failed transactions?

Research scope and limitations

Requested incident: widespread PHP-related shutdowns reported on 21 October 2026, confirmed by the commissioning user. Reporting window: that complete calendar day in Europe/London, with the 20 October advance warning included as context. Sources were retrieved on 22 October. Living pages may retain untimed edits; no historical snapshot was available to certify every sentence as it stood at midnight. No later dated outcome is incorporated.

Dutch original-language sources were read and translated into English. Ten primary-source records support the report. The case selection demonstrates breadth without claiming comprehensive coverage. No geographic incidence rate, global outage count or financial total is calculated.

Prior-edition check: mailbox results identified a 21 October report titled "UK infrastructure outages and possible links". Its full contents were not reviewed, so subject overlap cannot be excluded. No prior PHP-specific issue was established; archive-wide deduplication remains incomplete.

Prepared as a new nominated-incident investigation. Email distribution of this report has not been requested.

SOURCE REGISTER

Sources 01–05

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

-
- 01 **News Archive 2026: advance notice, security advisory and fixed releases**
PHP project · 20 and 21 October 2026
Family: Software maintainer / original release · Accessed 22 October 2026. Full relevant entries; English. Living archive; original publication times not shown. Technical cause and fixed versions are vendor findings.
<https://www.php.net/archive/2026.php>
-
- 02 **Critical security issue affecting PHP**
UK National Cyber Security Centre · 21 October 2026
Family: UK authority / vendor-informed guidance · Accessed 22 October 2026. Full alert; English. Retrieved version includes post-release advice; no separate update timestamp shown.
<https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php>
-
- 03 **Security Advisory 2026-018: Critical Vulnerabilities in PHP**
CERT-EU · 21 October 2026; v1.0 and v1.1 same date; displayed release 15:20:18, timezone unspecified
Family: EU institutional security / vendor-informed guidance · Accessed 22 October 2026. Full advisory; English. Release timing is attributed to CERT-EU; exploitation likelihood is an assessment, not a victim finding.
<https://cert.europa.eu/publications/security-advisories/2026-018/>
-
- 04 **Aantal websites Rijksoverheid preventief offline na kwetsbaarheden PHP**
Government of the Netherlands · 21 October 2026, 15:13 local displayed; update untimed
Family: Government service-impact announcement · Accessed 22 October 2026. Full Dutch page; translated by ISS Global. Confirms named precautionary suspensions; no exact start/end times. Living update.
<https://www.rijksoverheid.nl/actueel/nieuws/2026/10/21/aantal-websites-rijksoverheid-preventief-offline-na-kwetsbaarheden-php>
-
- 05 **Blijf op de hoogte van de PHP-kwetsbaarheden**
NCSC Netherlands · 21 October 2026, 11:03; updates 14:30, 15:50 and 20:40 displayed
Family: Dutch authority / own service status · Accessed 22 October 2026. Full Dutch community notice; translated by ISS Global. Later update headings do not repeat the date; read in the dated incident context.
<https://community.ncsc.nl/p/php>
-

SOURCE REGISTER

Sources 06–10

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

-
- 06 Temporary service interruption
ASIMUT / Dennis Jung Møller · 21 October 2026; metadata 14:53:36 +02:00
Family: Independent operator / direct suspension statement · Accessed 22 October 2026. Full English notice. Recovery estimate is conditional, not confirmation of restoration or exact downtime.
<https://asimut.com/news/temporary-service-interruption/>
-
- 07 Service Notice: Potential Website Outages Due to Critical PHP Vulnerabilities
Georgetown University Information Services · 21 October 2026
Family: Independent university operator / direct response statement · Accessed 22 October 2026. Full English notice. Confirms affected-server isolation; potential service effects; no list or completion timestamp.
<https://uis.georgetown.edu/uis-announcement/service-notice-potential-website-outages-due-to-critical-php-vulnerabilities/>
-
- 08 Critical vulnerabilities in PHP: Install security updates immediately
Swiss National Cyber Security Centre · 21 October 2026
Family: Swiss authority / vendor-informed guidance · Accessed 22 October 2026. Full English official page. Advisory and verification guidance; not evidence of a Swiss service outage.
<https://www.bacs.admin.ch/en/warnung-php-en>
-
- 09 Critical PHP update on Wednesday, October 21, 2026 (14:00 UTC) - PSA-2026-10-20
Drupal Security Team · Displayed date 21 October 2026; identifier contains 20 October
Family: Application ecosystem / host responsibility guidance · Accessed 22 October 2026. Full English notice. Publication uses displayed date, not identifier. Does not confirm a Drupal.org outage.
<https://www.drupal.org/psa-2026-10-20>
-
- 10 Critical Vulnerabilities in PHP (PHP2Shell), CC-4875
NHS England Digital · 21 October 2026, 15:51 displayed; last edited same time
Family: Health-sector security authority / threat assessment · Accessed 22 October 2026. Full English alert. Demonstrated exploitation and forecast risk are distinct from a confirmed NHS compromise or outage.
<https://digital.nhs.uk/cyber-alerts/2026/cc-4875>
-