

CRITICAL · ACTIVELY EXPLOITED

# PHP2Shell: Critical PHP Vulnerabilities Under Active Exploitation

Two flaws in PHP itself let an attacker with no password take control of a web server. Part A tells business leaders what to ask for today. Part B gives IT teams the detail to act.

|                                                                                      |                                                                |                                                                              |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>ISSUED BY</b><br>Cybersecurity Working Group,<br>CIO-CXO Digital Leadership Forum | <b>SEVERITY</b><br>Critical, CVSS v4.0 9.2. Actively exploited | <b>DATE</b><br>22 October 2026                                               |
| <b>VULNERABILITIES</b><br>CVE-2026-109618<br>CVE-2026-109619                         | <b>REFERENCE</b><br>CIO-CXO/CSWG/SA/2026/001                   | <b>CLASSIFICATION</b><br>TLP:CLEAR. Share freely within member organisations |

## SUMMARY

### At a glance

PHP2Shell is two critical flaws in PHP, the technology behind most websites, including WordPress, Joomla, Drupal, Magento and Laravel sites. One crafted request lets an attacker with no password run code on the web server and steal passwords and keys. Attacks began on **17 October 2026**, four days before disclosure; fixes were released on **21 October**. Because the flaw is in PHP itself, an up-to-date website is still exposed until the PHP beneath it is patched.

## PART A For CEOs and Business Owners

*No technical knowledge needed*

### 01

#### You are probably exposed

A website, portal, online shop or payment page very likely runs on PHP, even if a developer or host manages it.

### 02

#### The business risk is real

Fraud, stolen customer data, downtime, lost trust and duties under the Data Protection and Privacy Act, 2019.

### 03

#### It is your decision

Responsibility stays with your organisation, not the vendor. Ask the question and get the answer in writing.

**About the Cybersecurity Working Group.** A standing group of the CIO-CXO Digital Leadership Forum that brings together CIOs, CISOs and senior security practitioners to issue advisories, share threat intelligence with CERT.UG and sector CERTs, and build private-sector cyber coordination. Led by **Andrew Omoding** (Team Lead; Manager, Information Technology Security, NSSF) and **Emmanuel Kasule** (Co-Lead; Manager Cybersecurity, Stanbic Bank), with **Elizabeth Busingye** (Secretary), **Moses Kutosi** (Finance) and **Arthur Bright Niwagaba** (Membership Lead; CEO, Acadia Infosec Solutions), supported by the Forum Secretariat under **Gideon Nkurunungi**, Executive Secretary.

## PART A · ACTION

## What to do this week

### 1 Ask today

Send your web developer, hosting provider or IT team this message:

*“Does our website, portal or app run on PHP? If so, has it been updated to a fixed version (8.5.12, 8.4.27, 8.3.36 or 8.2.35) or the vendor’s patched package? Please confirm in writing, with the date.”*

### 2 Get it in writing within 48 hours

If a system cannot be fixed quickly, instruct that it be restricted or taken offline until it is.

### 3 Run a quick, safe self-check (optional)

These free tools only read the PHP version your site shows publicly and do not attack it. “Vulnerable” means act now; “inconclusive” does not mean safe, so ask your provider.

[SOCRadar PHP2Shell Checker](#)[Brandefense PHP2Shell Check](#)

### 4 Ask for a compromise check

Attacks began before the fix existed, so ask your provider to check for signs of intrusion since 17 October and to change passwords and keys if anything looks wrong.

### 5 Report, and stay safe

Report suspected incidents to CERT.UG, UG-CERT or the Forum (contacts on page 3). Only check websites you own, avoid unfamiliar “checker” sites, and never download exploit code circulating online.

Hand Part B of this advisory to your IT team or provider



## PART B

## For IT and Security Teams

Technical detail for system owners, developers, hosting providers and security teams.

**CVE-2026-109618**

Memory corruption when PHP runs out of memory while request data is only partially initialised.

**Unauthenticated remote code execution**

**CVE-2026-109619**

Use-after-free: data from one request is reused by a later request on the same worker.

**Remote code execution and memory disclosure**

**Affected:** every PHP installation serving web requests, including PHP-FPM, Apache mod\_php (highest risk: the exploit runs before application code), php-cgi, FrankenPHP and LiteSpeed. Distribution packages may keep the old version number, so check your vendor’s advisory, and do not miss PHP in control panels, containers, appliances, Windows servers and test sites.

**17 Oct**

First exploitation observed, before public disclosure

**20 Oct**

Details leaked; PHP announces an emergency release

**21 Oct**

Fixes released; widespread attacks reported

## Fixed versions

| Branch     | Fixed in | Action                                   |
|------------|----------|------------------------------------------|
| 8.5.x      | 8.5.12   | Upgrade                                  |
| 8.4.x      | 8.4.27   | Upgrade                                  |
| 8.3.x      | 8.3.36   | Upgrade                                  |
| 8.2.x      | 8.2.35   | Upgrade                                  |
| 7.4 to 8.1 | None     | Vendor build, source backport or upgrade |
| 5.4 to 7.3 | No fix   | Upgrade or remove from internet          |

## Temporary mitigations

Server or pool level only, then restart all workers.

**109619:** `session.upload_progress.enabled=0` ; PHP 8.5 also `fatal_error_backtraces=0` ; PHP-FPM consider `pm.max_requests=1`

**109618:** `memory_limit=-1` at admin level; strict request size limits; block unused multipart uploads; container memory limits

These buy time; they are not a fix. Restore normal limits once patched.

## Action plan

### PRIORITY 1

#### Within 24 hours

- Inventory all PHP, including third-party hosted systems
- Upgrade or install patched packages; rebuild containers
- Restart workers and confirm the patched version runs
- Restrict or take offline what cannot be patched; enable WAF

Lead: IT operations and security

### PRIORITY 2

#### Within 48 hours

- Written patch confirmation from every vendor and host
- Begin the compromise review from 17 October

Lead: CIO, vendor management

### PRIORITY 3

#### Within 7 days

- Authenticated scans
- Rotate credentials where compromise is suspected
- Reverse temporary settings
- Report to the Working Group and CERT.UG

Lead: security, risk and compliance

## Signs of compromise since 17 October

- Worker crashes, segfaults or out-of-memory errors in web and PHP-FPM logs
- Large, nested or malformed POST and multipart requests
- New or changed PHP files, especially in upload and cache folders
- New scheduled tasks, accounts or SSH keys; unexpected outbound connections or shells

## Detection and response

Tenable (369483), Qualys (QID 389102) and Rapid7 have authenticated checks. Searchlight Cyber's open-source php2shell-scanner actively probes and can crash workers: use only on systems you are authorised to test. If compromised, rotate every reachable secret and consider notifying the PDPO and your sector regulator.

## Who to contact

### NATIONAL CERT

#### CERT.UG/CC

National Information Technology Authority, Uganda (NITA-U)

🌐 [www.cert.ug](http://www.cert.ug)

✉ [info@nita.go.ug](mailto:info@nita.go.ug)

☎ 0326 555 700 · +256 785 807 169

### SECTOR CERT

#### UG-CERT

Uganda Communications Commission (UCC)

🌐 [www.ucc.co.ug](http://www.ucc.co.ug)

✉ [info@ug-cert.ug](mailto:info@ug-cert.ug)

☎ +256 414 339 100

### FORUM MEMBERS

#### CIO-CXO Forum Secretariat

For the Cybersecurity Working Group

🌐 [www.cio-cxo.africa](http://www.cio-cxo.africa)

✉ [secretariat@cio-cxo.africa](mailto:secretariat@cio-cxo.africa)

☎ 0394 538 616

InfoSec and CISOs: join the Working Group

[forms.cloud.microsoft/r/3b6mZcLmrc](https://forms.cloud.microsoft/r/3b6mZcLmrc)



Join the CIO-CXO Digital Leadership Forum

[www.cio-cxo.africa/membership](http://www.cio-cxo.africa/membership)

