

# PHP2Shell — Biomed Tech Briefing

Oct 22, 2026 · @hey you

## At a glance

PHP2Shell is two critical flaws in PHP (CVE-2026-109618 and CVE-2026-109619) that let an attacker take over a web server remotely, with no login and no user click. PHP runs a large share of web servers and web-based admin portals, potentially including some in our clinical environment. Patches came out on October 21, 2026, and attackers are already trying to exploit it.

| Item                   | Detail                                                                              |
|------------------------|-------------------------------------------------------------------------------------|
| CVEs                   | CVE-2026-109618 (out-of-memory corruption),<br>CVE-2026-109619 (stale global state) |
| Severity               | Critical — 9.2 (CVSS v4.0, PHP security team); 9.8 (CVSS v3.1, NVD)                 |
| Login needed?          | No                                                                                  |
| Result if exploited    | Attacker runs their own code on the server                                          |
| Exploited in the wild? | Yes, per several security vendors; not yet on CISA KEV                              |
| Patch available?       | Yes, for PHP 8.2–8.5 only                                                           |

## Why it matters to Biomed

PHP often sits quietly inside the systems we support, and vendors rarely advertise it. If one of these is taken over, an attacker can steal or alter data, knock the system offline, or use it as a stepping stone into other hospital networks.

Places PHP commonly hides:

- Vendor device management and configuration servers
- Medical device middleware and data aggregation servers
- Asset tracking and equipment management portals

- Built-in web login pages on appliances and gateways
- Virtual machines and containers a vendor supplied and maintains

## Affected and fixed versions

Every PHP version from 5.4 through 8.5 is affected. Only the four currently supported branches have a fix; anything at 8.1 or older stays vulnerable and needs isolation or replacement.

| PHP branch | Vulnerable     | Fixed in                    |
|------------|----------------|-----------------------------|
| 8.5        | 8.5.0 – 8.5.11 | 8.5.12                      |
| 8.4        | 8.4.0 – 8.4.26 | 8.4.27                      |
| 8.3        | 8.3.0 – 8.3.35 | 8.3.36                      |
| 8.2        | 8.2.0 – 8.2.34 | 8.2.35                      |
| 5.4 – 8.1  | All versions   | No fix — isolate or migrate |

Vendors sometimes backport fixes into older version numbers, so a vendor bulletin overrides the table for their product.

## What should BME do?

1. **Flag web-managed systems.** Any device, server or appliance with a web login page — send it to the Biomed Cybersecurity Team so we can check whether it runs PHP.
2. **Don't patch vendor systems without validation.** Updates must come through the vendor so the system stays validated and supported.
3. **Report odd behaviour.** Slowdowns, crashes, unexpected restarts or unfamiliar files on a device server — report it right away.
4. **Pass on vendor contact.** If a vendor reaches out about PHP2Shell, forward it to the team.

## What's in the news

Security vendors report active exploitation attempts, and healthcare is among the targeted sectors; whether attacks are succeeding widely is still unclear.

| Date   | Source                         | What happened                                                                                                                  |
|--------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Oct 22 | <a href="#">Sansec</a>         | Mass exploitation now looks less likely: public exploits fail on a default PHP install and mostly need a second bug in the app |
| Oct 22 | <a href="#">Check Point</a>    | 10% of organizations worldwide saw exploitation attempts; healthcare and medical at 13%                                        |
| Oct 22 | <a href="#">Brandefense</a>    | Neither CVE is yet on the CISA Known Exploited Vulnerabilities list                                                            |
| Oct 21 | <a href="#">watchTowr</a>      | Honeypots caught exploitation of both CVEs in the wild                                                                         |
| Oct 21 | <a href="#">PHP / SOCRadar</a> | Patches released at 14:00 UTC                                                                                                  |
| Oct 20 | <a href="#">SecurityWeek</a>   | Details leaked ahead of planned disclosure                                                                                     |

The main attack path runs through PHP's Session Upload Progress feature, which is on by default. Turning it off ( `session.upload_progress.enabled = off` ) is the common stopgap until a patch is applied.

No PHP2Shell alert from most medical device manufacturer was found as of this date; watch for these over the coming days.

#### Manufacturer's Websites checked as of 22 Oct 2026:

- Philips - has a notice that they are investigating but no additional info - likely going to be published on In-Centre
- Siemens - No Information
- GE Healthcare - No Information
- Medtronic - No Information
- Stryker - No Information
- Hologic - No Information
- SpaceLabs - No Information
- ECRI - No Information

## Sources

- VulnBrief Intelligence Reports: CVE-2026-109618 and CVE-2026-109619 (generated Oct 22, 2026)
- [Canadian Cyber Center](#)
- [PHP2Shell — Wikipedia](#)
- [watchTowr — PHP2Shell intelligence](#)
- [SOCRadar — affected versions and fix](#)
- [Brandefense — fixed versions](#)
- [Sansec — PHP2Shell research](#)
- [Check Point — impact update](#)
- [SecurityWeek — leak report](#)
- [php2shell-checker — vulnerable version ranges](#)