illumio

PHP2Shell Fact Sheet

PHP2Shell is a pair of critical flaws in the PHP engine, patched on October 21, 2026.[1] They let attackers run code on web servers without logging in. Here's how the attack works, who is affected and what to do.

9.2[1]
Critical severity score out of 10 (CVSS v4.0)

0[1]
Logins needed to attack a vulnerable server

22.6M[4]
Exposed instances found that may be vulnerable

69%[5]
Of websites with a known back end run on PHP

IN PLAIN LANGUAGE

PHP runs most of the web, including some of its most popular sites, like Wikipedia, and platforms such as WordPress, Drupal and Joomla.[2,5] These bugs sit inside the engine itself, so an attacker can strike before your website's own code or login checks even run.

How the break-in works

2 UP CLOSE

Two ways PHP trips

CVE-2026-109618

The half-built request

A crafted upload makes PHP run out of memory mid-request. Cleanup then acts on half-built data the attacker shaped, corrupting memory so it runs their code.[3]

CVE-2026-109619

The leftovers

PHP keeps pointing at memory it already freed. The attacker's next request on that worker refills it with their data, which PHP trusts, leaking memory or running code.[3]

1



Knock

The attacker sends one specially built web request to your server.

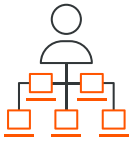
2



Trip

PHP fumbles its memory before your app even sees the request.

3



Take over

The attacker runs commands on the web server as if they owned it.

4



Wander

Next stop: your databases, file shares and other servers. Unless the way is blocked.

Steps 1 to 3: patching locks the front door. Update PHP and they stop working — for now.

Step 4: Illumio Insights spots the move. **Illumio Segmentation** locks the inside doors.

Are you exposed?

Almost certainly, if you run PHP on a web server. Every version since 5.4 is affected, on PHP-FPM, Apache mod_php, php-cgi, FrankenPHP and LiteSpeed alike.[1] Find your version:

5.4–7.3	7.4–8.1	8.2	8.3	8.4	8.5
No fix coming	Source patch only	Get 8.2.35	Get 8.3.36	Get 8.4.27	Get 8.5.12

Stuck on 7.4–8.1? Apply PHP's minimal source patch, or ask your Linux distribution or support vendor for a backported fix.[1,2]

How it unfolded

Researchers at Calif and Wiz both used AI models in their work. Wiz says frontier AI turned a long-standing flaw into a working exploit.[1,3]

OCT 20
The CVE numbers leak online. PHP moves its security release up a day.[1,2]

OCT 21, 14:00 UTC
PHP ships fixes for 8.2 through 8.5.[1]

OCT 21
Cloudflare and watchTowr report early attacks. The story is still developing.[1]

Your to-do list

- [ ] **Map it**
  List every PHP install, including ones hiding inside vendor software, control panels and CMS platforms.
- [ ] **Segment it**
  Let each PHP server reach only the systems it needs, and block its outbound internet. If one server is breached, the attacker can't spread.
- [ ] **Patch it**
  Upgrade now.[1] It stops the bleeding, but not the next flaw.
- [ ] **Shield it or isolate it**
  Can't patch yet? Apply the PHP security team's official mitigations, which reduce exposure to specific attack paths. They're only a stopgap, so also keep the server off the internet or behind a VPN or web application firewall.[6]
- [ ] **Observe it**
  Watch for PHP starting shells or tools like curl and wget. Look for new files in the web root and new accounts or cron jobs.[2]

1. Tenable, PHP2Shell FAQ, Oct. 21, 2026. Cites PHP's advisories.
2. Huntress, PHP2Shell: leaked critical PHP vulnerabilities, Oct. 20, 2026.
3. Help Net Security, PHP2Shell vulnerabilities patched, Oct. 21, 2026.
4. Unit 42, Threat Brief: Critical Vulnerabilities in PHP, Oct. 21, 2026.
5. W3Techs, Usage statistics of PHP, Oct. 21, 2026.
6. PHP security team, security advisory, php.net, Oct. 21, 2026.

Details current as of Oct. 21, 2026. Links are clickable in the PDF.

Patching matters.
Resilience rooted in Zero Trust matters more.

See how Illumio contains breaches like PHP2Shell before they spread.

Visit Illumio.com

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters. Recognized as a Leader and Customer Favorite in The Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2026 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.