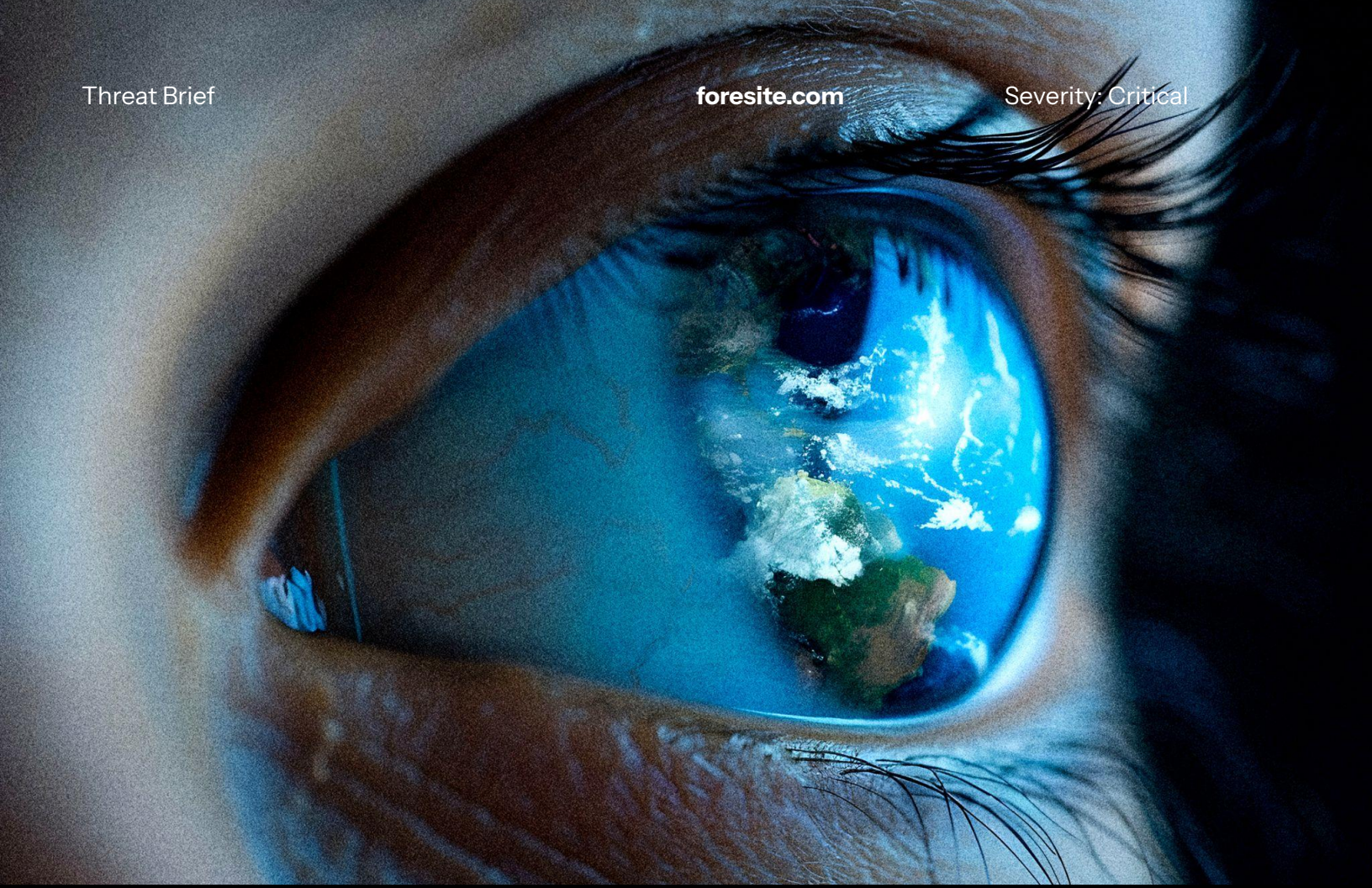




CVE-2026-109618 and CVE-2026-109619

Unauthenticated remote code execution in the PHP core. Patch now, then confirm no one got in.

Threat Brief: PHP2Shell



At a glance

CVEs	CVE-2026-109618 and CVE-2026-109619 (PHP2Shell)
Severity	Critical, CVSS v4.0 9.2 each
Impact	Unauthenticated remote code execution on the web server
Affected	Every PHP installation serving web requests, including PHP-FPM, Apache mod_php, php-cgi, FrankenPHP and LiteSpeed. mod_php carries the greatest risk
Fixed versions	PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35, released October 21, 2026
End of life	PHP 8.1 and earlier receive no official fix. Source backports exist for 7.4, 8.0 and 8.1, and some Linux and LTS vendors provide patched packages
Exploitation	Exploitation attempts reported. Public proof-of-concept code exists. Large-scale exploitation expected

Summary

On October 20, details of two critical PHP vulnerabilities known as PHP2Shell leaked ahead of coordinated disclosure. They let an attacker take control of a web server with a single unauthenticated request, before any application code runs. PHP released emergency fixes on October 21. Because the flaws sit in the PHP core, every application built on it inherits the risk, including WordPress, Drupal, Joomla, Magento, Laravel and hosting platforms. Foresite assesses PHP2Shell as a critical, high-likelihood threat.

Technical details

- CVE-2026-109618, RCE via out-of-memory corruption: out-of-memory handling can leave request data partially initialized, which cleanup then treats as valid.
- CVE-2026-109619, RCE via stale global state: request state can survive after its memory is freed and be reused by a later request on the same worker.

Exploitation happens in the interpreter before application code runs, so plugin updates and application-level controls do not protect against it.

Threat brief: PHP2Shell



Threat landscape and recommended actions

Threat landscape

- Cloudflare and Patchstack reported exploitation attempts on October 21, and public proof-of-concept code exists.
- Palo Alto Networks Unit 42 counts 22.6 million exposed instances that are potentially vulnerable.
- Government services in the Netherlands and elsewhere in Europe were taken offline as a precaution.
- Neither CVE is yet in the CISA Known Exploited Vulnerabilities catalog. Foresite expects that to change.

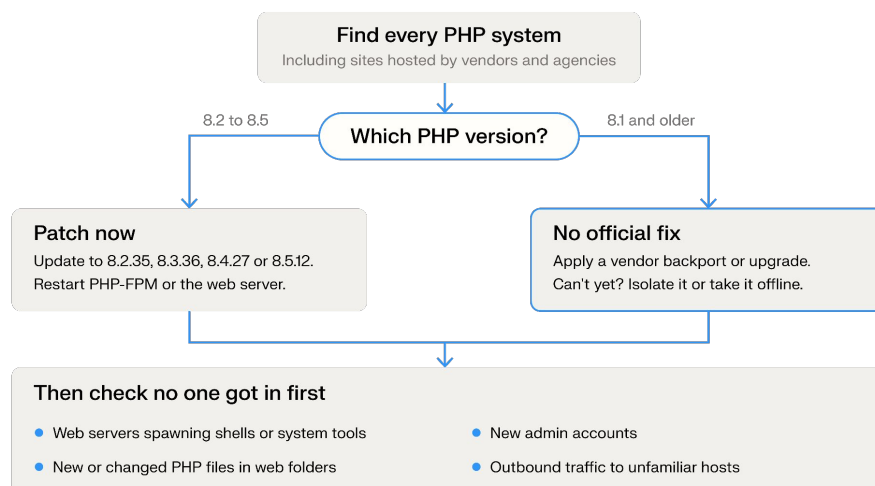
Payment environments are a priority target. An exposed self-hosted store can carry a hidden card skimmer on its checkout page, turning a vulnerability into a PCI incident.

Recommended actions

1. Identify every system running PHP, including websites hosted by third-party providers, agencies and vendors.
2. Patch all supported versions to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, prioritizing internet-facing and payment systems. Restart PHP-FPM or the web server so the patched interpreter loads.
3. For PHP 8.1 and earlier, apply a vendor backport or upgrade to a supported release. If neither is possible right away, isolate the system or take it offline.
4. After patching, check no one got in first: web shells, new or modified PHP files, new administrator accounts and unusual outbound connections from web servers.
5. Review checkout and payment pages for unfamiliar scripts or recently changed files.
6. Contact Foresite right away if anything looks unusual.

PHP2Shell: what to do, in order

CVE-2026-109618 and CVE-2026-109619, patched October 21, 2026



Patching is the only complete fix. WAF rules and interim settings buy time.

foresite.com

Threat brief: PHP2Shell



Interim protection, detection and our response

If you cannot patch today

Patching is the only complete fix. These reduce risk until patches are applied:

- Place PHP sites behind a WAF with PHP2Shell rules. Cloudflare rules are available on all plans.
- Palo Alto Networks firewalls with Advanced Threat Prevention can block attacks using Threat Prevention signature 543004.
- Apply PHP's interim guidance, including a low `post_max_size` and, on PHP 8.5, `fatal_error_backtraces = 0`.
- Restrict or remove internet access to PHP systems that cannot be patched.

Do not rely on the `session.upload_progress` workaround that circulated before the patch. It does not match the published root cause.

Detection and hunting

- Web server processes (php-fpm, apache2, httpd, nginx) spawning command shells or system utilities.
- New or modified PHP files in web directories, especially in upload or cache folders.
- Sudden spikes in PHP memory exhaustion errors, fatal errors, worker crashes or segmentation faults in web server logs.
- New administrator accounts and outbound connections from web servers to unfamiliar destinations.

What Foresite is doing

- Notified customers with payment processing environments first, followed by the full customer base.
- Tracking guidance from PHP, government agencies and research partners, and validating new information before acting on it.
- Building and validating detections for exploitation and post-exploitation activity with our technology partners.
- Updating vulnerability scanning as vendor definitions are released, and supporting customers through patching and end-of-life decisions.

Want a second set of eyes? Book a free PHP2Shell exposure review at **foresite.com**.

Sources: PHP security advisories GHSA-w8hw-w9fx-j79w and GHSA-6wmf-4rv5-p3rp. Unit 42. Help Net Security. Patchstack. CERT-EU Advisory 2026-018, UK NCSC and NCSC-NL. Sansec, and SecurityWeek, October 20 to 21, 2026.