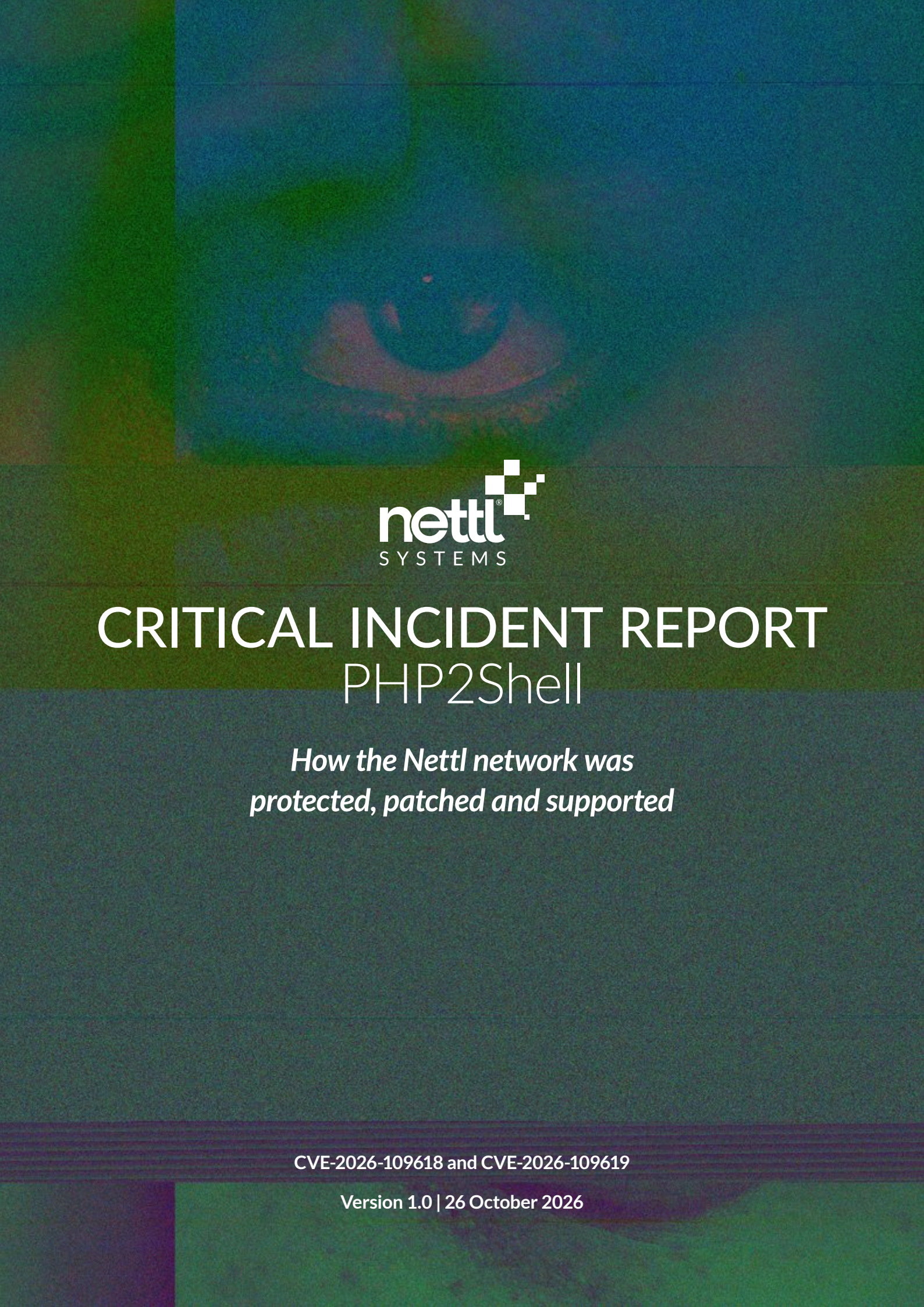


nettl SYSTEMS

CRITICAL INCIDENT REPORT
PHP2Shell

How the Nettl network was protected, patched and supported

CVE-2026-109618 and CVE-2026-109619

Version 1.0 | 26 October 2026

AT A GLANCE

Incident Two critical remote code execution flaws in PHP

Severity 9.2 out of 10 (critical)

Scope Thousands of partner and client websites on Nettl hosting

First reported attacks 08:45, Wednesday 21 October

Protective measures in place 10:05, Wednesday 21 October

All hosted sites patched 04:38, Thursday 22 October

Sites taken offline None

Compromises detected None

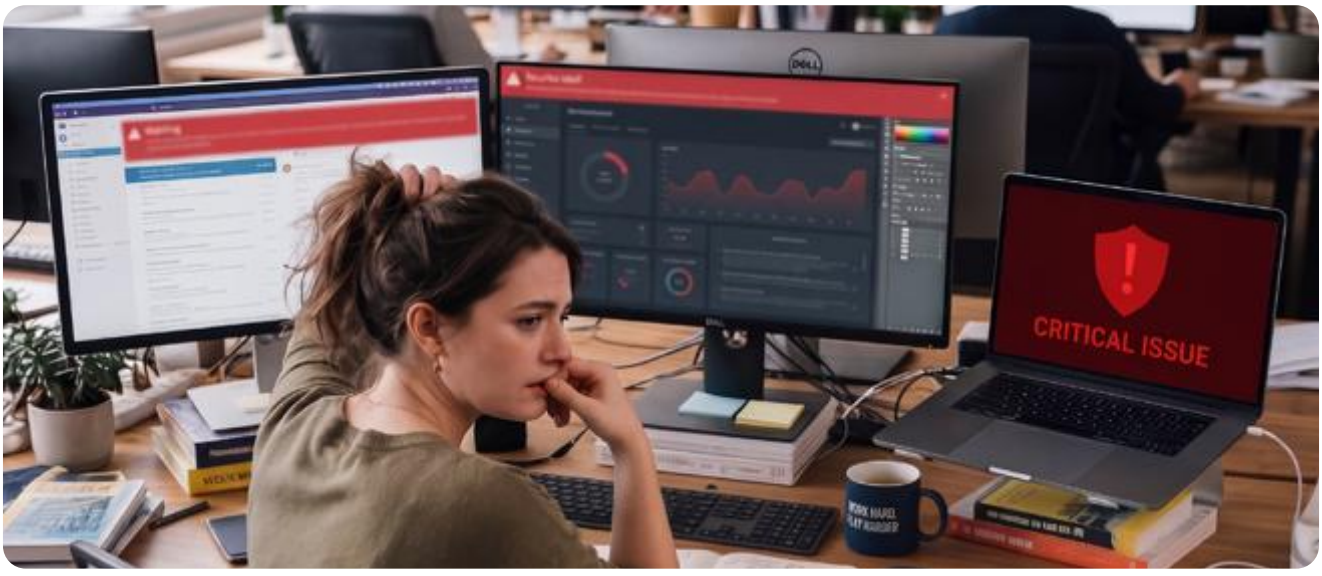
Action required from partners None

1. SUMMARY

On 20 October 2026, details of two critical flaws in PHP were leaked ahead of their planned disclosure. PHP runs most of the world's websites, including every WordPress site, and the flaws could allow an attacker to take control of the server a website runs on.

Attacks were reported the following morning, hours before an official fix existed. Organisations around the world responded by taking websites offline. Some hosting providers told their customers to apply patches or upgrade PHP themselves.

Nettl took a different approach. We contained the threat across the network by 10:05 on 21 October without taking any site offline, patched every PHP version on our servers overnight, and kept partners informed at every stage. All hosted sites were patched by 04:38 on 22 October. Our monitoring shows no evidence of any compromise, and no action was required from partners or their clients.







2. THE INCIDENT

PHP2Shell is the name given to two vulnerabilities in PHP itself (CVE-2026-109618 and CVE-2026-109619), rather than in a single plugin, theme or application. Both were rated 9.2 out of 10 for severity.

Details were posted online before PHP's security team was ready to release a fix, giving attackers a head start. PHP announced the flaws at 20:35 on 20 October. Cloudflare reported the first attacks at 08:45 on 21 October, and PHP released the official fix at 15:00 that afternoon.

The response elsewhere shows how seriously the threat was taken. Government departments, airlines and Wikipedia took systems offline while they patched, and a PHP core developer advised that businesses able to switch servers off for a day should do so.

3. OUR RESPONSE

3.1 Containing the threat without taking sites offline

The flaws were exploited through file uploads. At 09:40 on 21 October, our management and development teams agreed to switch off uploads across the whole network rather than take sites dark. The block was in place on every hosted site by 10:05.

Websites stayed online and visible to their visitors throughout. The only temporary change was that file uploads were unavailable until patches were in place.

3.2 Patching every PHP version, not forcing upgrades

A common response from hosting providers was to tell customers to upgrade to the latest version of PHP, such as PHP 8.4, to receive the fix. That is a reasonable position. In practice, though, a PHP upgrade can break themes, plugins and custom code, and the testing and fixing that follows takes time partners and their clients did not have during an active threat.

We chose instead to apply the security fix to every version of PHP available on our servers, including older versions. Every site stayed on the version it already ran, now with the fix in place. Partners had nothing to upgrade, test or repair.

Once the Nettl System itself was updated at 17:05, our developers rolled the patches out across our hosting through the night. Every hosted site was patched by 04:38 on 22 October.

3.3 Response timeline

○ INCIDENT ● PROTECTION ● COMMUNICATION

Tue 20 Oct

○ **20:35** PHP's security team announces two critical flaws

Wed 21 Oct

● **08:15** Nettl developers begin tracking the threat

○ **08:45** Cloudflare reports the first attacks

● **09:00** Developers start applying available updates

● **09:40** Decision taken to switch off uploads across the network

● **10:05** Uploads disabled on every hosted site; no sites taken offline

● **10:40** Critical incident topic opened in the Arena

● **11:05** Incident email to all partners; direct contact with web-focused partners in the UK, US, the Netherlands, New Zealand and Australia

● **14:05** Second incident email: fix expected at 15:00

○ **15:00** PHP releases the official fix

● **17:05** Nettl System updated; rollout across hosting begins

Thu 22 Oct

● **04:38** **All hosted sites patched**

● **11:25** Third incident email with a full rundown of the changes

● **12:55** New Arena topic with guidance on updating older PHP versions

"Our System Development team acted early, communicated constantly and worked through the night. Because of that, thousands of small business websites stayed online and protected, with nothing for their owners to do."

Chris Lowe, Managing Director, Nettl Systems Ltd

4. PARTNER COMMUNICATION

Our aim was for partners to hear from us before their clients started asking questions, and to have answers ready when they did.

- **The Arena.** A critical incident topic went live at 10:40 on 21 October, giving the whole network one place for updates.
- **Email.** Three incident emails went out over two days, at 11:05 and 14:05 on 21 October and 11:25 on 22 October.
- **Direct contact.** Partners whose businesses rely heavily on web work were contacted individually, across the UK, US, the Netherlands, New Zealand and Australia.
- **Response times.** Between 10:40 and 14:00 on 21 October, every question raised in the Arena, by email or through the Geek channel was answered within 15 minutes.
- **Oodles.** The AI in the Nettl System was briefed so partners could get accurate answers at any moment.
- **Client conversations.** Partners were given verified news sources and talking points to share with their own clients.
- **Follow-up.** At 12:55 on 22 October, a new Arena topic gave guidance on updating older PHP versions.





5. OUTCOME AND IMPACT

5.1 Security

Our development team has monitored all systems and the hosting infrastructure for partner and client sites throughout and since the incident. In their update to the network, they confirmed:

“We’ve got no evidence in our monitoring logs that there have been any compromises related to the recent events.”

At the time of their update, the team was aware of attempted attacks globally but no reports of a successful attack on any site. Monitoring continues.

5.2 Service

- No hosted site was taken offline at any point.
- File uploads were temporarily unavailable while the protective block was in place.
- Every site remained on its existing PHP version, so no theme, plugin or custom code changes were needed.
- No action was required from partners or their clients.

6. GUIDANCE: KEEPING SITES UP TO DATE

The overnight patch protected each site on the PHP version it already ran. Moving to a current, supported version of PHP remains best practice, but upgrades are not always straightforward, because themes, plugins and custom code can break.

Following the incident, Nettl offered partners two routes for upgrading their sites.

Self-managed upgrade. Partners can upgrade PHP themselves at no charge. If anything breaks afterwards, Nettl's development team will investigate. Fixes under five minutes are free, and anything longer is quoted for time and cost before work starts.

Nettl Care Plan. Nettl upgrades PHP, tests the site and fixes anything that breaks as part of the plan. From then on, core, theme and plugin updates are handled, regular backups allow a rollback if needed, and security monitoring and uptime checks catch problems early. Care Plan sites also receive priority technical support. When the next vulnerability like this one appears, those sites are already covered.

7. WHAT WE ARE CARRYING FORWARD

- **Contain, don't close.** Switching off the targeted feature kept every site online. We will look for the same option first in future incidents.
- **Patch in place.** Fixing each PHP version where it runs avoids forcing upgrades on partners under pressure.
- **Communicate early and often.** One Arena topic, regular emails and fast replies kept the network informed before clients asked.
- **Listen to the network.** Partners raised ideas for handling PHP updates in future. These are being discussed in the Arena and will inform our approach.
- **Keep watching.** Monitoring of all systems and hosting infrastructure continues.



8. QUESTIONS



Partners: For general updates, follow the incident topic in the Arena.
For anything specific to your sites, raise a Geek ticket and our team will pick it up.

For external questions, press and media requests, please email marketing@nettl.com.
If you are interested in joining the community, contact partner@nettl.com.

9. ABOUT NETTL

Nettl is a network of independent web, print, design and signage studios, backed by the Nettl System: the operating system for creative businesses. Partners run their own studios, either under the Nettl brand or using the Nettl System with their own.

The Nettl System brings client management, workflow, finance, website building and hosting, print and signage pricing, and digital marketing services together in one place. Oodles, the AI built into the system, helps keep work moving. Partners also get expert-led training and support, and a community of studios across the world, including the UK, Ireland, the Netherlands, the US, New Zealand and Australia.

Nettl Systems is part of Software Circle PLC. Find out more at partner.nettl.com.











Nettl Systems Ltd, a division of Software Circle plc. Registered in England No. 272 8004
Registered Address: C/o Gateley Legal, Ship Canal House, 98 King Street, Manchester, United Kingdom, M2 4WU