

ALERT

CYBERSECURITY & DATA PROTECTION

Critical PHP flaws: every day without patching weakens your *legal defense.*

PHP runs nearly 7 in 10 websites, including every WordPress site. Two critical flaws are already being exploited.

01 · WHAT HAPPENED

Three flaws in *four days*.

CRITICAL · CVSS 9.2

EXPLOITED

PHP2Shell

CVE-2026-109618 · CVE-2026-109619

Fixed on October 21 in PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35.

PHP 8.1 and earlier will not be patched: you must upgrade.

NARROW · OCTOBER 23

NO PATCH YET

CVE-2026-115560

No fix until the next regular release. Block it at the server level with

```
session.upload_progress.enabled=0
```

02 · THE RISK

On an unpatched server, an attacker *can*:

01 Get in without a password

Run their own code on your server.

02 Read your databases

Client files, employee data and stored passwords.

03 Stay *inside*

Leave hidden backdoors that stay active after you patch.

04 Turn your site against others

Infect your visitors, take your site down or attack third parties from your server.

03 · YOUR LEGAL EXPOSURE · MEXICO'S LFPDPPP

When the fix is free and available, not applying it is *hard to justify*.

Duty of security (art. 18): safeguards must reflect the risk and the state of technology.

FINES OF UP TO

\$37.5

million Mexican pesos

320,000 UMA (Mexico's fine unit) for a database security breach attributable to you (arts. 58-XI and 59).

 $\times 2$

with sensitive data

+

additional fine if the violation persists

04 · OTHER CONSEQUENCES

Beyond the *fine*:

Ex officio inspection

ART. 54

Mexico’s Anti-Corruption and Good Governance Ministry may open one on well-founded grounds to presume a violation.

Immediate notice to data subjects

ART. 19

If the breach significantly affects their property or moral rights.

Compensation

ART. 53

Affected individuals may claim damages.

Civil or criminal liability

ART. 61

Administrative penalties do not preclude it.

What to do *this week*

1 Get it in writing

Ask whoever runs your servers to confirm they updated PHP (or upgraded to 8.2 or later) and applied the configuration change.

2 Preserve the logs

Have them reviewed and preserved from October 17, the date of the first detected exploitation attempt.

3 Assess notice to data subjects

If there are signs of unauthorized access, decide right away whether you must notify them.

4 Document every step

That record is your evidence of due diligence.

Need to assess your exposure or
review your *vendor contracts*?

cyber@lipp.legal

