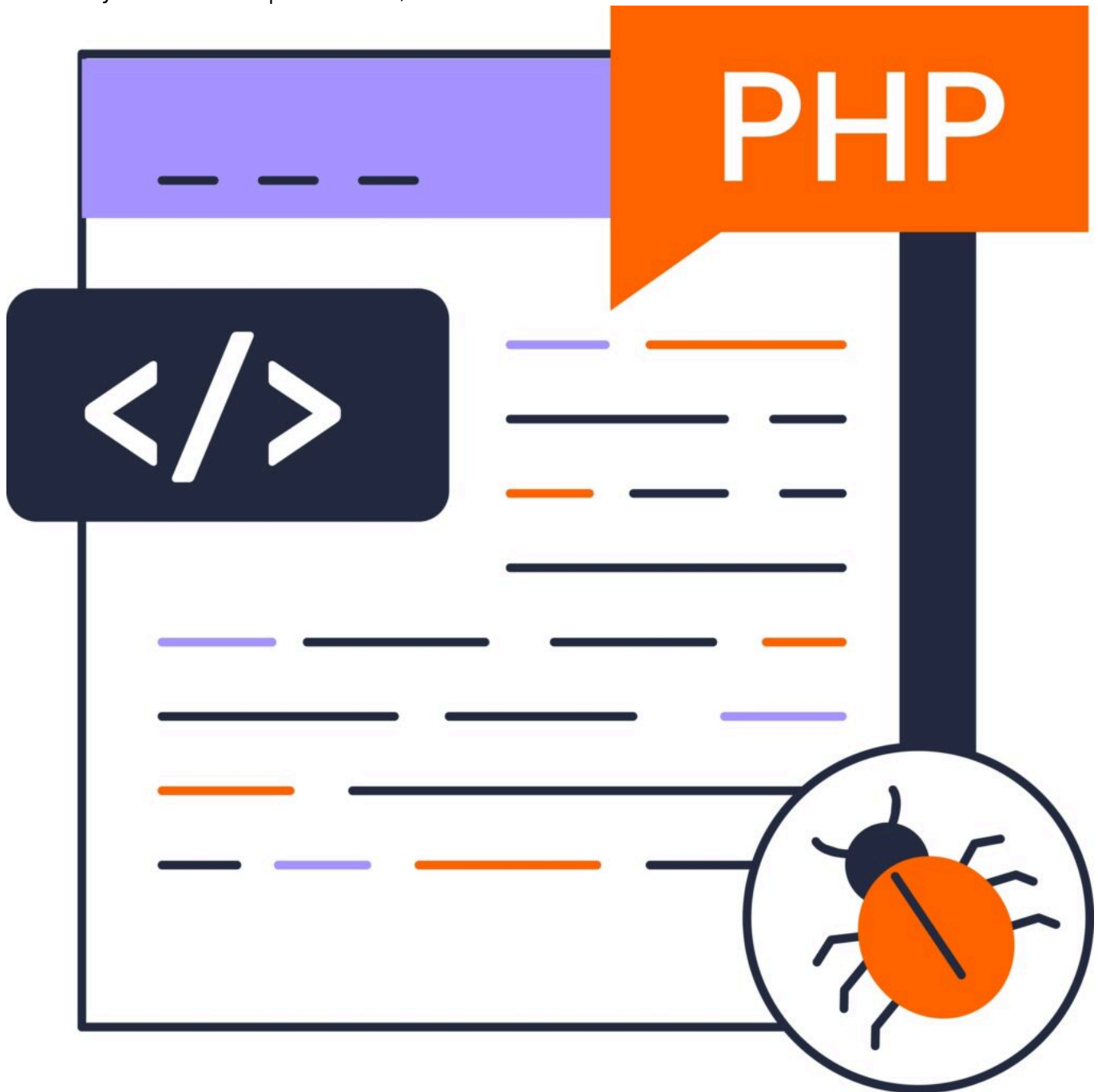


PHP SECURITY FLAW POSSIBLE IN 70% OF WEBSITES - LEGAL RISKS OF NOT PATCHING

Category: Infrastructure and Telecommunications, IT Law, Technology Law
written by Lucien Pierce | October 23, 2026



What is PHP?

PHP (PHP Hypertext Preprocessor) is a software tool used to design websites. Critical [security issues](#) have been identified. These security vulnerabilities could allow attackers to easily access and [control affected web servers](#), enabling them to steal sensitive data, install malware or cause even greater damage. The PHP flaw is possible in 70% of websites and there are legal risks in not patching

How was it discovered?

Wiz, a cloud and AI security service provider, used an AI tool to identify the software security vulnerabilities. It highlights that PHP is used by [70% of the world's websites](#), so there is a strong chance that it powers your organisation's website. Prudent organisations, such as the [Finnish and Dutch governments](#), have taken public-facing internet services offline.

It's prevalent across organisations processing sensitive information

When it comes to South African organisations, it is likely that many government departments and entities run websites using software that relies on PHP. This is because the [government's website guidelines](#) recommend tools such as WordPress, Drupal and Joomla. These three tools are specifically mentioned as being at the [core of the identified software vulnerabilities](#).

This means that public-facing government websites, such as those of the Department of Home Affairs (<https://www.dha.gov.za/index.php/notices>), the National Department of Health (https://knowledgehub.health.gov.za/lms/login/forgot_password.php), the Department of Communications and Digital Technologies (<https://www.dcdt.gov.za/index.php>), the South African Police Service (<https://www.saps.gov.za/careers/careers.php>) and the power utility – Eskom (eskomcareers.ci.hr/applicant/index.php), may all have security vulnerabilities.

What are the legal implications?

Given that the security vulnerability has been [widely publicised](#), any organisation that has not acted reasonably (meaning speedily) to address the security vulnerability, places itself in a risky legal position. If it suffers some sort of breach and personal or confidential information is stolen, or worse still its operations are affected, it may not be able to rely on some of the defences that are usually available in commercial contracts. Worse still, it is not likely to have any defence when it comes to its statutory obligations under laws like the Protection of Personal Information Act (POPIA).

If an organisation is unable to meet its contractual obligations, relying on [a defence such as an Act of God](#) (force majeure) is unlikely to succeed. By now, all responsible organisations with capable information security departments should have taken the necessary steps to mitigate these security risks. If customers suffer damage because of an organisation's failure to act, they may have good prospects of succeeding in a damages claim against it.

To make matters worse, the organisations will most likely not be able to call on their cybersecurity insurance policies, because their insurers are certain to repudiate on the basis that they failed to act reasonably, namely apply the required security patches, or take their websites offline until the patch could be applied.

Organisations still using PHP based website tools would do well to act fast, or face the consequences.

About the author: Lucien Pierce is a specialised technology and privacy attorney and a director at PPM Attorneys, with over 25 years of experience in telecommunications, data protection, cybersecurity and emerging technology law. Contact him at www.ppmattorneys.co.za.