

Php2Shell – Critical PHP Vulnerability Discovery

This Loss Prevention Standard discusses the background to a recently discovered software scripting language vulnerability and provides helpful guidance to help identify and manage the associated cyber risks.

Php2Shell – Critical PHP Vulnerability Discovery

Introduction

A pair of critical vulnerabilities have been discovered and released in the scripting language, PHP. PHP is used on a large portion of websites across the internet, and running a vulnerable version of this may allow attackers to execute commands remotely, without having to authenticate.



Background

Two critical security flaws, given the identifiers CVE-2026-109618 and CVE-2026-109619 and collectively nicknamed “PHP2Shell”, were publicly disclosed on 21 October 2026. Both are rated as critical severity. They affect the core PHP software itself, not any website or app built on it, which means the risk applies broadly across almost any system running PHP. Many well-known platforms have been affected or taken down for maintenance in the hours following the discovery, including government and infrastructure websites around the world.

These flaws could allow an attacker to take control of a web server from the outside, without needing a username, password, or any existing access. Since the vulnerabilities became public, there have already been real attempts to exploit them. This is considered an active, live threat.

What Could an Attacker Do?

If a system is left unpatched, a successful attack could allow someone to:

- Run their own commands on the server, effectively taking it over.
- Access sensitive data stored or processed by the website, such as customer information or login details.
- Install hidden backdoors to maintain access even after the issue is later fixed.
- Use the compromised server as a stepping stone to attack other systems.

Affected Versions

All versions of PHP from 5.4 through to 8.5 are affected. Fixes have been released for current, supported versions:

- PHP 8.5 — fixed in version 8.5.12
- PHP 8.4 — fixed in version 8.4.27
- PHP 8.3 — fixed in version 8.3.36
- PHP 8.2 — fixed in version 8.2.35

Any system running PHP 8.1 or older is considered unsupported and will not receive a fix and should be treated as a priority for upgrading to a newer, supported version.

Practical Next Steps

1. Identify which of your public-facing websites or systems run on PHP, and which version. Consider use of external scanning and asset discovery tools, such as Shodan and Censys. Review your domains and consider websites built on PHP based platforms, such as Wordpress, Magento and others. Servers may also be configured to not show the PHP version, so consider this is not foolproof. Confirm with the manager of the server what version is being run.
2. Where the version is out of date, apply the relevant update listed above as soon as possible.
3. Where a system is running an unsupported version (8.1 or older), plan to upgrade it to a current version rather than waiting for a patch.
4. After updating, double-check that the new version is live, particularly for larger setups with multiple servers, where an old version can sometimes be missed.

This is being actively exploited in the wild and as such should be treated as urgent and handled ahead of routine update schedules.

Contact Information

Canada

Please visit [Aviva Risk Management Solutions | Aviva Canada](#) or email us at arms.canada@aviva.com

Ireland

Please visit [Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland](#) or Email us at armsireland@aviva.com

United Kingdom

Please visit [Aviva Risk Management Solutions](#) or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

Note: These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

The following Specialist Partners provide products or services in relation to risk guidance provided, discussed or referenced in this Loss Prevention Standard.

Canada

For more information please visit: [Our Specialist Partner Network | Aviva Canada](#)

Ireland

For more information please visit: [Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland](#)

United Kingdom

- Cyber security services - [CSA Cyber](#)

For more information please visit: [Aviva Risk Management Solutions - Specialist Partners](#)

Standards, Sources and Useful Links

- [Critical security issue affecting PHP | National Cyber Security Centre](#)
- [PHP: News Archive - 2026](#)

Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Cyber - Respond and Recover.**
- **Cyber - Supply Chain Risk Management**
- **Cyber - Ransomware**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**
- **Cyber - 12 Top Tips to Protect Against Cyber Attacks**
- **Cyber - Security Certifications for Organisations**
- **Cyber - Back-ups**
- **Cyber - Playbooks**

Please visit [Loss Prevention Standards](#) to view the full library.

Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Relevant courses include:

- **Cyber Fundamentals**
- **Social Engineering**

Please visit [Aviva Risk Training Solutions](#) for further guidance.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. By extension, any links to third-party websites do not constitute marketing by Aviva and are included solely for the reader's information and educational purposes. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

22nd October 2026

Version 1.0

ARMSGI5242026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.