



Critical PHP2Shell Vulnerabilities (CVE-2026-109618 & CVE-2026-109619)

23 October 2026

TLP:CLEAR

PHP2SHELL Advisory

This advisory is relevant to all Samoan individuals, IT managers and organisations. This alert is intended to be understood by technical audiences.

What is it?

SamCERT is advising all organisations operating PHP-based web applications and services to urgently assess and remediate two critical vulnerabilities collectively known as PHP2Shell.

What is the issue?

PHP is the programming language behind many of the world's websites. Many government, business and community websites in Samoa run on PHP, either on their own servers or through a hosting provider.

Two critical vulnerabilities, collectively known as PHP2Shell ([CVE-2026-109618](#) & [CVE-2026-109619](#)), have been found in PHP itself. They allow an attacker to take control of a web server without needing a username or password, by sending specially crafted web requests.

Attackers could run their own code on the server, steal sensitive information such as passwords, access tokens and API keys, or take the website offline. Websites can be affected even if their own application code is secure.

SamCERT is advising all organisations operating PHP-based web applications and services, you need to be **aware of these vulnerabilities** and **urgently implement the security advice**.

Recommended Actions

1. Identify all PHP installations across the organization
2. **Patch immediately** to one of the following versions or later:
 - PHP 8.5.12
 - PHP 8.4.27
 - PHP 8.3.36
 - PHP 8.2.35
3. Apply vendor-provided updates for bundled or embedded PHP deployments
4. Where immediate patching is not feasible, organisations should consider isolating internet-facing resources from public networks until the fix is applied and verified.

Upgrading PHP is the only complete remediation.

PHP has released a fix for the vulnerability. See [vendor advisory](https://www.php.net/archive/2026.php#2026-10-21-5) <https://www.php.net/archive/2026.php#2026-10-21-5>

If you have been affected by a cyber incident or require further information contact SamCERT on:



www.samcert.gov.ws/report-incident



samcert@mcit.gov.ws



+685 26 117

TLP:CLEAR