Regulatory Authority of Curaçao

ADVISORY ON PHP VULNERABILITY

OCTOBER 22, 2026

TLP: GREEN

BACKGROUND

PHP is a widely used server-side programming language that supports the development and operation of websites and web applications. It is commonly used to process information, interact with databases, and enable essential functionalities, including user authentication, online transactions, and electronic forms.

Given its widespread use across public and private digital infrastructure, vulnerabilities affecting PHP may expose organizations to significant cybersecurity risks, particularly where affected systems are accessible through the Internet.

ISSUE

RAC/CARICERT draws attention to two critical security vulnerabilities affecting PHP that may enable unauthenticated remote code execution (RCE) under certain conditions.

Successful exploitation could allow unauthorized parties to execute malicious code on affected systems, potentially compromising the confidentiality, integrity, and availability of information and digital services.

RAC/CARICERT strongly advises organizations operating PHP-based websites and applications to assess their exposure without delay and implement recommended mitigation measures.

VULNERABILITIES

The following vulnerabilities have been identified:

1. **RCE via Out-of-Memory (OOM) Corruption, CVE-2026-109618 (GHSA-w8hw-w9fx-j79w)**

This vulnerability relates to the handling of out-of-memory conditions, which may interrupt PHP processes while internal request data remains partially initialized. Subsequent cleanup operations may incorrectly process invalid data, potentially creating conditions for remote code execution.

2. **RCE via Stale Global State, CVE-2026-109619 (GHSA-6wmf-4rv5-p3rp)**

This vulnerability involves internal request-related information remaining accessible after its associated memory has been released. Subsequent requests processed by the same worker may interact with this outdated information, potentially creating conditions for remote code execution.

These vulnerabilities are collectively referred to as PHP2SHELL.

SYSTEMS AT RISK

Organizations operating internet-facing PHP-based websites and applications may be exposed where affected PHP versions or configurations are in use.

The risk may be heightened where systems are not adequately maintained, security updates have not been applied, or appropriate cybersecurity controls are absent.

RAC/CARICERT emphasizes that timely vulnerability management, system maintenance, and the implementation of recommended cybersecurity safeguards are essential to reducing exposure and protecting the reliability of digital services.

RECOMMENDED MITIGATION MEASURES

In view of the potential severity of these vulnerabilities, RAC/CARICERT strongly recommends that system administrators, IT service providers, and organizations operating affected systems take the following measures as a matter of priority:

1. **Assess exposure**: identify PHP-based systems and determine whether affected versions or configurations are in use.

2. **Apply security updates**: update affected installations to PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35, as applicable, subject to confirmation of the relevant security releases.

3. **Consult software vendors**: organizations using Linux distributions or long-term support (LTS) solutions should verify the availability and application of vendor-provided security patches.

4. **Address unsupported versions**: PHP 8.1 and earlier versions are no longer supported by the PHP project. Organizations should migrate to supported versions or verify the availability of appropriate vendor-maintained security fixes.

5. **Monitor for suspicious activity**: review relevant system and application logs for indicators of potential exploitation and investigate anomalies promptly.

6. **Maintain incident response readiness:** ensure that appropriate procedures are in place to identify, contain, and respond to suspected security incidents.

Where immediate remediation is not feasible, organizations should assess the associated risks and implement appropriate interim safeguards until the vulnerabilities can be adequately addressed.

REPORTING AND FURTHER INFORMATION

RAC/CARICERT encourages organizations to remain vigilant and promptly report suspected exploitation or related cybersecurity incidents. Timely reporting contributes to improved situational awareness, coordinated incident response, and the protection of Curaçao's digital infrastructure.

SOURCES

https://www.php.net
https://cert.europa.eu/publications/
https://community.ncsc.nl

For questions or to report incidents, please contact us at:

General inquiries : info@caricert.cw | info@rac.cw
Incident reporting : cert@caricert.cw
Website : caricert.cw | rac.cw

Published by RAC / CARICERT
Regulatory Authority of Curaçao / National Cyber Emergency Response Team