# NOTA MAKLUMAN CSIRTNS BILANGAN 3 TAHUN 2024
# 13 JUN 2024

## ISU/ANCAMAN

Ancaman *Critical RCE Flaw in PHP* - **CVE-2024-4577**

## PENGENALAN

Satu ancaman keselamatan kritikal dalam perisian PHP telah dikenal pasti oleh seorang penyelidik keselamatan[1] pada 7 Jun 2024 dan telah diterbitkan dalam MITRE CVE[2] (CVE-2024-4577) pada 9 Jun 2024.

Ancaman ini memberi kesan kepada versi PHP 8.1.* < 8.1.29, 8.2.* < 8.2.20, dan 8.3.* < 8.3.8 yang menggunakan Apache dan PHP-CGI pada sistem Windows.

Ancaman ini berlaku apabila sistem menggunakan kod tertentu yang menyebabkan Windows menggantikan aksara dalam *command line* yang dihantar ke *Win32 API functions*. Ini boleh menyebabkan modul PHP-CGI salah mentafsir arahan tersebut dan **membolehkan pengguna berniat jahat menjalankan kod berbahaya atau mendedahkan kod sumber skrip**.

## IMPAK

Sebarang *code* boleh dijalankan pada pelayan (server) yang mempunyai kerentanan ini dengan teknik *argument injection attack*.

Kerentanan ini melibatkan **semua versi PHP yang dipasang pada sistem operasi Windows**. Sila rujuk jadual di bawah untuk butiran lanjut:

- PHP 8.3 < 8.3.8 (terdedah kepada kerentanan)
- PHP 8.2 < 8.2.20 (terdedah kepada kerentanan)
- PHP 8.1 < 8.1.29 (terdedah kepada kerentanan)

Versi PHP 8.0, PHP 7 dan PHP 5 telah mencapai akhir hayat (End-of-Life).

**Semua versi pemasangan XAMPP pada Windows terdedah kepada kerentanan ini secara *default installation*[3].**

## SASARAN

Laman sesawang, sistem dalam talian, rangkaian dan aplikasi Kerajaan.

## CADANGAN TINDAKAN PENGUKUHAN

1. Pentadbir sistem berkaitan disyorkan untuk mengemaskini kepada versi terkini PHP iaitu 8.3.8, 8.2.20 dan 8.1.29.
2. Memandangkan PHP CGI adalah satu fungsi yang *outdated*, disyorkan juga untuk menggunakan fungsi yang lebih selamat seperti Mod-PHP, FastCGI atau PHP-FPM.

3. Penggunaan XAMPP untuk persekitaran *production* adalah tidak dibenarkan. Pentadbir disarankan untuk menaiktaraf aplikasi berkaitan ke persekitaran yang lebih selamat.

**RUJUKAN**

[1] https://blog.orange.tw/2024/06/cve-2024-4577-yet-another-php-rce.html

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4577

[3] https://arstechnica.com/security/2024/06/php-vulnerability-allows-attackers-to-run-malicious-code-on-windows-servers/

**MAKLUMAT LANJUT**

*Cyber Security Incident Response Team* Negeri Sembilan (CSIRTNS)
Bahagian Teknologi Maklumat
Tingkat 3, Blok B, Wisma Negeri, 70503 Seremban, Negeri Sembilan
Tel : +606-7659890; Faks : +606-7627760
E-Mel : certn9@ns.gov.my