مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in PHP

Tracking #:432315939
Date:10-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Critical Remote Code Execution Vulnerability in PHP that could be exploited to execute malicious code on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Description:

- **CVE-2024-4577**
- **CVSS Score:** 9.8 Critical
- A critical remote code execution (RCE) vulnerability exists in PHP installations running with CGI mode enabled. This vulnerability arises from improper character encoding handling, specifically due to the interaction between PHP and the "Best Fit" feature of Windows encodings. Malicious actors can exploit this vulnerability to execute arbitrary code on affected servers, potentially leading to complete system compromise.
- The vulnerability stems from an oversight in PHP's handling of character encoding conversions when running in CGI mode on Windows. The "Best-Fit" feature in Windows can be leveraged by attackers to bypass protections implemented for a similar vulnerability (CVE-2012-1823). This bypass allows for arbitrary code injection.
- Publicly available exploit code exists for CVE-2024-4577

Affected Systems:

- All versions of PHP for Windows are vulnerable, including:
  - Supported versions (PHP 8.3, 8.2, 8.1)
  - End-of-life versions (PHP 8.0, 7.x, 5.x)
- XAMPP installations on Windows are particularly susceptible due to their default CGI mode configuration.

Fixed Versions:

- PHP 8.3.8
- PHP 8.2.20
- PHP 8.1.29

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by PHP

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-4577