مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Chartify WordPress Plugin

Tracking #:432316514

Date:15-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in the Chartify WordPress plugin, which is actively being exploited by attackers in the wild.

TECHNICAL DETAILS:

A critical vulnerability has been discovered in the Chartify WordPress plugin (**CVE-2024-10571**), which is actively being exploited by attackers in the wild. This vulnerability affects all versions of the Chartify plugin up to and including version 2.9.5, and it allows unauthenticated remote attackers to exploit a local file inclusion (LFI) flaw via the 'source' parameter. This flaw can enable attackers to inject arbitrary files and execute malicious PHP code on affected websites, potentially compromising the site's integrity and security.

The vulnerability has been assigned a CVSS score of 9.8, making it a critical issue. Exploits are actively being blocked, with 2,207,540 attacks reported by Wordfence in just 24 hours, indicating that malicious actors are aggressively targeting vulnerable sites.

Affected Versions:

- Chartify <= 2.9.5

Fixed Version:

- Chartify 2.9.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected plugin to the latest version at the earliest.

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://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/chart-builder/chartify-wordpress-chart-plugin-295-unauthenticated-local-file-inclusion-via-source