مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Anti-Spam by CleanTalk WordPress Plugin

Tracking #:432316559
Date:26-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in the Anti-Spam by CleanTalk WordPress plugin that could allow unauthenticated attackers to install malicious plugins and execute malicious code on vulnerable websites.

TECHNICAL DETAILS:

Two critical vulnerabilities have been identified in the Anti-Spam by CleanTalk WordPress plugin, which is installed on over 200,000 websites. These vulnerabilities, tracked as CVE-2024-10542 and CVE-2024-10781, allow unauthenticated attackers to install malicious plugins and execute arbitrary code on affected sites. Both vulnerabilities have a CVSS score of 9.8, indicating their critical severity.

Vulnerabilities Details:

CVE-2024-10542: Authorization Bypass via Reverse DNS Spoofing

- This vulnerability is due to an authorization bypass caused by reverse DNS spoofing. The plugin determines the IP address using the X-Client-Ip and X-Forwarded-By header parameters, which can be manipulated by attackers. This allows them to bypass authentication checks and remotely install and activate plugins.
- Unauthenticated attackers can gain control over the site by installing arbitrary plugins, potentially leading to remote code execution if another vulnerable plugin is present.
- **Affected Versions:** Up to 6.43.2

CVE-2024-10781: Authorization Bypass due to Missing Empty API Key Check

- This vulnerability arises from the absence of checks for empty API keys, allowing unauthorized access when the API key is not configured.
- Attackers can perform unauthorized actions such as plugin installation and activation without authentication.
- **Affected Versions:** Up to 6.44

Fixed Versions:

- Anti-Spam by CleanTalk plugin version 6.45 or later

RECOMMENDATIONS:

- **Implement regular updates**: Establish a routine for updating all WordPress plugins and themes.
- **Use a Web Application Firewall (WAF)**: This can provide an additional layer of protection against various attacks.
- **Monitor website activity**: Regularly check for any suspicious behavior or unauthorized changes.

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/blog/2024/11/200000-wordpress-sites-affected-by-unauthenticated-critical-vulnerabilities-in-anti-spam-by-cleantalk-wordpress-plugin/