مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of XSS Vulnerabilities in WordPress Plugins

Tracking #:432315914

Date:03-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed active exploitation of high-severity unauthenticated stored Cross-Site Scripting (XSS) vulnerabilities in various WordPress plugins.

TECHNICAL DETAILS:

Active exploitation attempts targeting high-severity unauthenticated stored Cross-Site Scripting (XSS) vulnerabilities (**CVE-2024-2194, CVE-2023-6961, and CVE-2023-40000**) in various WordPress plugins. These vulnerabilities allow attackers to inject malicious scripts into websites, potentially creating new administrator accounts, installing backdoors, and setting up tracking scripts

Vulnerability: Unauthenticated Stored XSS (Cross-Site Scripting)
Affected Software: Various WordPress Plugins with CVEs: CVE-2024-2194, CVE-2023-6961, and CVE-2023-40000
Attack Payload: Injects a script tag that points to an obfuscated JavaScript file for malicious actions like creating administrator accounts, installing backdoors, and setting up tracking scripts.

Indicators of Compromise:
Attached Excel Sheet

RECOMMENDATIONS:

- Update Vulnerable Plugins: If a plugin is found to be vulnerable, update it to the latest patched version as soon as possible. If an update is unavailable, consider deactivating or removing the plugin until a patch is released.
- Review Administrator Accounts: Monitor for unauthorized administrator accounts and disable any suspicious ones.
- Implement Web Application Firewall (WAF): Consider implementing a WAF to help prevent XSS attacks by filtering out malicious code before it reaches your website.
- Maintain Strong Passwords: Enforce strong and unique passwords for all WordPress accounts, especially administrator accounts.
- Stay Informed: Subscribe to security advisories from WordPress and relevant security vendors to stay updated on the latest threats.

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:

1. https://nvd.nist.gov/vuln/detail/CVE-2024-2194
2. https://www.tenable.com/cve/CVE-2023-6961
3. https://nvd.nist.gov/vuln/detail/CVE-2023-40000