



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity XSS Vulnerability in WordPress Core
Tracking #:432315818
Date:06-05-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity vulnerability in the WordPress core, specifically within the Avatar block which could allow both authenticated and unauthenticated attackers to execute malicious scripts, potentially leading to full site control.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **Vulnerability ID:** CVE-2024-4439,7.2 HIGH
- **Affected Versions:** WordPress Core versions up to 6.5.2
- **Vulnerability Type:** Stored Cross-Site Scripting (XSS)
- **Impact:** Potential compromise of website, including data theft, defacement, and malware distribution.

Affected Versions: 6.5 – 6.5.1, 6.4 – 6.4.3, 6.3 – 6.3.3, 6.2 – 6.2.4, 6.1 – 6.1.5, 6.0 – 6.0.7

Fixed Versions: Versions: 6.1.6, 6.2.5, 6.3.4, 6.4.4, 6.5.2

RECOMMENDATIONS:

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

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://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-security-release/>