



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Joomla Content Management System

Tracking #:432315643

Date:23-02-2024

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 Multiple Vulnerabilities in Joomla Content Management System that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Joomla, a popular content management system, has recently addressed multiple vulnerabilities that could lead to remote code execution (RCE) attacks due to cross-site scripting (XSS) flaws.

Vulnerabilities Details:

- CVE-2024-21722: MFA management features not properly terminating existing user sessions.
- CVE-2024-21723: Inadequate parsing of URLs leading to open redirects.
- CVE-2024-21724: Inadequate input validation for media selection fields causing XSS vulnerabilities.
- CVE-2024-21725: Inadequate escaping of mail addresses resulting in XSS vulnerabilities.
- CVE-2024-21726: Inadequate content filtering within the filter code leading to multiple XSS vulnerabilities.

Affected Versions:

- CVE-2024-21722- Joomla! CMS versions 3.2.0-3.10.14-elts, 4.0.0-4.4.2, 5.0.0-5.0.2
- CVE-2024-21723-Joomla! CMS versions 1.5.0 - 3.10.14-elts, 4.0.0-4.4.2, 5.0.0-5.0.2
- CVE-2024-21724-Joomla! CMS versions 1.6.0 - 3.10.14-elts, 4.0.0-4.4.2, 5.0.0-5.0.2
- CVE-2024-21725-Joomla! CMS versions 4.0.0-4.4.2, 5.0.0-5.0.2
- CVE-2024-21726-Joomla! CMS versions 3.7.0-3.10.14-elts, 4.0.0-4.4.2, 5.0.0-5.0.2

Fixed Versions:

Joomla versions 5.0.3 and 4.4.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Joomla.

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://www.joomla.org/announcements/release-news/5904-joomla-5-0-3-and-4-4-3-security-and-bug-fix-release.html>
2. <https://developer.joomla.org/security-centre/925-20240201-core-insufficient-session-expiration-in-mfa-management-views.html>



3. <https://developer.joomla.org/security-centre/926-20240202-core-open-redirect-in-installation-application.html>
4. <https://developer.joomla.org/security-centre/927-20240203-core-xss-in-media-selection-fields.html>
5. <https://developer.joomla.org/security-centre/928-20240204-core-xss-in-mail-address-outputs.html>
6. <https://developer.joomla.org/security-centre/929-20240205-core-inadequate-content-filtering-within-the-filter-code.html>