مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Drupal Core

Tracking #:432316543

Date:21-11-2024

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Drupal Core that could potentially be exploited to execute malicious code on vulnerable systems.

TECHNICAL DETAILS:

A critical cross-site scripting (XSS) vulnerability exists in Drupal 7 core's Overlay module. This vulnerability allows attackers to execute malicious scripts in users' browsers under certain circumstances

Vulnerability Details:

- **Drupal Core - Cross-Site Scripting Vulnerability (SA-CORE-2024-005)**
- Severity: Critical
- The Overlay module in Drupal 7 core fails to properly sanitize user input, leading to a reflected cross-site scripting vulnerability. This vulnerability can be exploited to execute arbitrary JavaScript code in the context of the victim's browser session
- Successful exploitation of this vulnerability could allow attackers to:
  - Steal sensitive information, including session tokens and cookies
  - Perform unauthorized actions on behalf of the victim
  - Modify the appearance of the website to conduct phishing attacks

Affected Versions:

- Drupal 7 versions prior to 7.102

Mitigations:

- For Drupal 7, update to Drupal 7.102 or later
- Sites may also disable the Overlay module to avoid the issue

Additional Notes:

- Drupal 10 and Drupal 11 are not affected by this vulnerability, as the Overlay module was removed from Drupal core in Drupal 8
- The vulnerability is only exploitable against users who have both the 'Access the administrative overlay' permission and the Overlay module enabled

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions 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.drupal.org/sa-core-2024-005