



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Drupal
Tracking #:432316362
Date:04-10-2024

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 that Drupal has released security updates to address an Access Bypass vulnerability in the Two-Factor Authentication (TFA) module.

TECHNICAL DETAILS:

Vulnerability Details:

- **SA-CONTRIB-2024-043- Two-factor Authentication (TFA) Access bypass**
- **Security risk:** Critical
- The Two-Factor Authentication (TFA) module for Drupal, has a critical vulnerability that could allow an attacker to bypass two-factor authentication and gain unauthorized access to a Drupal site. This vulnerability occurs due to the module's failure to properly migrate sessions before prompting for a second factor token.
- While the vulnerability is mitigated by the requirement for an attacker to gather additional information and present a valid token, it still poses a significant risk, especially in environments with sensitive data.
- **Affected versions:** <1.8.0

Fixed versions:

- Two-factor Authentication (TFA) module for Drupal 8+ upgrade to Two-factor Authentication (TFA) 8.x-1.8
- Two-factor Authentication (TFA) module for Drupal 7 upgrade to Two-factor Authentication (TFA) 7.x-2.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions Released by Drupal.

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-contrib-2024-043>