

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Access Bypass Vulnerability in Drupal Email TFA
Tracking #:432317954
Date:06-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in the Email TFA module for Drupal, which could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

A moderately critical access bypass vulnerability has been identified in the Email TFA module for Drupal. The flaw could allow authenticated users with valid credentials to partially bypass email-based two-factor authentication requirements under specific conditions.

Vulnerability Details

Email TFA - Moderately critical - Access bypass - SA-CONTRIB-2025-115

- The vulnerability stems from incomplete enforcement of two-factor authentication during certain login workflows. While the module is intended to require email-based verification after password entry, a logic flaw allows a user with valid credentials to authenticate without completing the 2FA step under specific conditions.
- This can result in a partial bypass of the 2FA mechanism, reducing the overall security posture of affected Drupal sites.
- Successful exploitation could lead to an attacker with valid credentials bypassing two-factor authentication, reducing account security and potentially enabling unauthorized access depending on account privileges.

Affected Versions

- Email TFA versions prior to 2.0.6

Fixed Version

- Email TFA 2.0.6 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest 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-2025-115>