



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical Access Bypass Vulnerability in AJAX Dashboard**  
Tracking #:432318522  
Date:05-03-2026

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 critical access bypass vulnerability has been identified in the AJAX Dashboard module for entity dashboards.

## TECHNICAL DETAILS:

A critical access bypass vulnerability has been identified in the AJAX Dashboard module for entity dashboards. This vulnerability allows unauthorized users to access the dashboard configuration page if the AJAX Dashboard: Entity Dashboards submodule is enabled. While attackers cannot modify the dashboards' content directly, they could enable or disable dashboards, potentially impacting administrative oversight and system operations.

### Vulnerability Details

- **Vulnerability Type:** Access Bypass
- **CVE Identifier:** CVE-2026-3527
- **Security risk:** Critical
- **Component:** AJAX Dashboard: Entity Dashboards submodule
- **Affected Versions:** AJAX Dashboard < 3.1.0
- **Fixed Version:** AJAX Dashboard 3.1.0

## RECOMMENDATIONS:

### Immediate Upgrade:

- Update AJAX Dashboard to fixed version or later.

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-2026-022>