

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerabilities in Drupal alogin and Admin LTE
Tracking #:432316809
Date:30-01-2025

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 critical vulnerabilities in the Drupal Authenticator Login Module and the Drupal Admin LTE Theme that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Critical-Severity Vulnerabilities:

Authenticator Login - Access bypass - SA-CONTRIB-2025-009

- The Authenticator Login module, which allows two-factor authentication via QR code, contains a critical access bypass vulnerability. The module fails to properly protect its custom paths, enabling users to access other users' two-factor configurations
- **Affected versions:** < 2.0.6
- **Solution:**
 - For alogin module 1.0.x: Upgrade to Authenticator Login 2.0.6 or later (1.0.x is now unsupported)
 - For alogin module 2.0.x: Upgrade to Authenticator Login 2.0.6 or later
 - For alogin module 2.1.x: No action required

Drupal Admin LTE theme - Unsupported - SA-CONTRIB-2025-010

- The Drupal Security Team has marked the Drupal Admin LTE theme as unsupported due to an unresolved known security issue
- **Affected versions:** *
- **Solution:** Uninstall the Drupal Admin LTE theme.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2025-009>
- <https://www.drupal.org/sa-contrib-2025-010>