مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Drupal Automated Logout Module

Tracking #:432318700

Date:01-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a cross-site request forgery (CSRF) vulnerability in the Drupal Automated Logout module. This issue could allow attackers to trigger unauthorized logout actions without user interaction.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-4393
- **Severity:** Moderately Critical
- **Vulnerability Type:** Cross-Site Request Forgery (CSRF)
- The Automated Logout module, which enables administrators to automatically log out users after a period of inactivity, does not adequately protect its routes against CSRF attacks. This weakness allows an attacker to craft malicious requests that can force users to be logged out without their consent, potentially disrupting user sessions and impacting availability.

Affected Versions

- Drupal Automated Logout module: <1.7.0 || >=2.0.0 <2.0.2

Fixed Versions

- For Automated Logout 8.x-1.x versions 8.x-1.6 or earlier, upgrade to version 8.x-1.7.
- For Automated Logout 2.x versions 2.0.1 or earlier, upgrade to version 2.0.2.

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-2026-030