مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in Drupal SAML SSO Module

Tracking #:432318465

Date:26-02-2026



**TLP: WHITE**

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the SAML SSO – Service Provider module for Drupal that may allow injection and execution of malicious scripts, potentially leading to session compromise, credential theft, or unauthorized actions.

## TECHNICAL DETAILS:

A critical cross-site scripting (XSS) vulnerability has been identified in the SAML SSO – Service Provider module for Drupal. The vulnerability occurs due to insufficient sanitization of user-supplied input, which may allow attackers to inject and execute malicious scripts. Successful exploitation could lead to session hijacking, credential theft, or unauthorized actions within affected Drupal sites.

**Vulnerability Details**

- **CVE-2026-3217**
- **Severity:** Critical
- The SAML SSO – Service Provider module enables SAML protocol-based single sign-on authentication for Drupal websites. The module does not properly sanitize certain user inputs, which may allow reflected cross-site scripting attacks. An attacker can potentially craft malicious links containing embedded scripts that execute when users interact with specially crafted requests.

**Affected Products**

- SAML SSO – Service Provider Drupal Module versions prior to 3.1.3

**Fixed Versions**

- SAML SSO – Service Provider 3.1.3 and 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-2026-018