مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Drupal SAML SSO - Service Provider

Tracking #:432318715

Date:03-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability in the SAML SSO – Service Provider module for Drupal. This flaw could allow unauthenticated attackers to gain unauthorized access to protected resources by bypassing the SAML authentication mechanism.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-5343
- **Vulnerability Type:** Authentication Bypass
- **Severity:** Critical
- The SAML SSO - Service Provider module does not properly enforce access restrictions during the authentication process. Specifically, insufficient validation or access control checks may allow an attacker to manipulate the authentication flow and bypass identity verification.
- Successful exploitation could allow attackers to:
  - Access protected areas without valid credentials
  - Impersonate legitimate users
  - Potentially gain administrative privileges depending on configuration

Affected Products

- **Drupal Module:** SAML SSO - Service Provider
- **Affected Versions:** All versions prior to 3.1.4

Fixed Versions

- SAML SSO - Service Provider 3.1.4 and later

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-2026-031