مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Drupal

Tracking #:432316227

Date:05-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Drupal released a security update addressing a critical security risk in its Paragraphs table.

TECHNICAL DETAILS:

A critical security risk was observed in Drupal's Paragraphs table. This module enables field collections to be displayed as tables. It supports display suite and field permissions and provides operations (modify, delete, duplicate). This module has multiple vulnerabilities due to the requirements on the routes it provides not being restrictive enough.

Vulnerability Details:

- **SA-CONTRIB-2024-036 | Security Risk: Critical**
  - **Information disclosure:** Several routes only checked for the 'access content' permission before displaying a paragraph, and did not check whether the user should actually have access to view the paragraph in question.
  - **Access bypass:** The paragraphs_item.add_page route previously allowed anyone with the 'access content' permission to add paragraphs to any content regardless of permissions to be able to edit the host field or content, or any other hooks for adjusting access to add paragraphs of that type.
  - **Affected Versions:** <1.23.0 || >=2.0.0 <2.0.2

Fixed versions:

- **For paragraphs_table 8.x-1.x:** Update to version 8.x-1.23.
- **For paragraphs_table 2.0.x:** Upgrade to version 2.0.2 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed 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-2024-036