



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Drupal POST File Module

Tracking #:432316513

Date:15-11-2024

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 a critical vulnerability in the Drupal POST File module that could potentially be exploited to gain unauthorized access and execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **SA-CONTRIB-2024-060- POST File - Cross Site Scripting, Arbitrary PHP code execution**
- Security Risk: **Critical**
- A critical security vulnerability exists in POST File module for Drupal, affecting versions prior to 1.0.2. This vulnerability could allow attackers to perform Cross-Site Scripting (XSS) attacks and execute arbitrary PHP code on affected systems.
- The POST File module creates an endpoint at /postfile/upload that accepts POST requests for uploading files into specified file systems (public, private, etc.). The vulnerability stems from the module's lack of proper file extension filtering, allowing the upload of potentially dangerous file formats. This behavior can bypass Drupal's allow_insecure_uploads configuration, potentially leading to severe security breaches.
- This vulnerability is mitigated by the fact that an attacker must have a role with the permission "postfile upload".
- Successful exploitation of this vulnerability could allow attackers to execute Cross-Site Scripting (XSS) attacks, upload and execute arbitrary PHP code, and potentially gain unauthorized access to the Drupal installation.

Fixed Versions:

- POST File module for Drupal 10.3.x/11.x, upgrade to POST File 1.0.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-060>