مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Drupal AI module

Tracking #:432316949

Date:07-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Drupal AI Automators module, a submodule of the AI (Artificial Intelligence) project that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **AI (Artificial Intelligence) - Critical - Remote Code Execution - SA-CONTRIB-2025-021**
- The AI Automators submodule, part of the Drupal AI module, allows users to create automated tasks that populate field data using Large Language Model (LLM) outputs. A critical vulnerability exists in the module's handling of user input within optional Automator Types.
- The module fails to sufficiently sanitize user-provided input before passing it to an underlying shell command. This oversight enables malicious actors to inject arbitrary commands, leading to Remote Code Execution (RCE) on the host system.
- Exploitation of this vulnerability could result in full compromise of the affected site, including unauthorized data access, modification, or server control.

Affected Configurations:

- Sites using the AI Automators submodule with optional Automator Types enabled.
- Drupal installations with the AI module versions prior to 1.0.5.

Fixed Versions:

- AI module version 1.0.5 or 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-2025-021