مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Drupal AI module

Tracking #:432316753

Date:16-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Drupal AI module that could be exploited to expose sensitive data, modify configurations, and execute severe actions, particularly with custom agents on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **AI (Artificial Intelligence) - Cross Site Request Forgery - SA-CONTRIB-2025-003**
- Severity: Critical
- A critical Cross-Site Request Forgery (CSRF) vulnerability exists in the Drupal AI module. This vulnerability is present in the AI Chatbot and AI Assistants API sub-modules, which allow users to interact with Drupal sites via a chat interface.
- The vulnerability stems from the AI Chatbot module's failure to implement proper CSRF protection in the Deepchat chatbot. This oversight could allow an attacker to craft scenarios that forge requests on behalf of privileged users. The potential impact of this vulnerability is severe, especially when combined with other AI sub-modules:
  - When used with the AI Search submodule, an attacker could potentially access indexed data they shouldn't have permission to view
  - In conjunction with the external AI Agent module, an attacker might expose and modify site configurations, including fields, content types, and vocabularies
- Sites with custom-built agents that have more privileged access may be at greater risk from this vulnerability.
- **Affected versions:** >1.0.0 <1.0.2

Mitigation:

- **Upgrade:** Install the latest version of the AI module (version 1.0.2 or later).
- **Uninstall:** If upgrading is not feasible, uninstall the AI Chatbot sub-module.

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-2025-003