مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical vulnerabilities in Drupal Opigno LMS

Tracking #:432316131
Date:08-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Critical vulnerabilities in Drupal Opigno Learning Management System (LMS) that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. **Opigno group manager (SA-CONTRIB-2024-027)**
   - A critical vulnerability exists in the Opigno group manager component that allows for arbitrary PHP code execution via an administrative form.
   - Exploitation of this vulnerability requires the attacker to have the "update group learning_path" permission and specific conditions within the system.
2. **Opigno module (SA-CONTRIB-2024-028)**
   - A critical vulnerability exists in the Opigno module component due to insufficient file validation, leading to potential Remote Code Execution (RCE) and Cross Site Scripting (XSS).
   - Exploitation of this vulnerability requires the attacker to have a role with the "create opigno tincan activities" permission.
3. **Opigno Learning path (SA-CONTRIB-2024-029)**
   - A critical vulnerability exists in the Opigno Learning Path module that allows for arbitrary PHP code execution and Cross Site Scripting (XSS) through malicious file uploads.
   - Exploitation of this vulnerability requires the attacker to have a role with the "Manage group content in any group" permission.

Impact

Successful exploitation of these vulnerabilities could result in:

- Complete compromise of the Opigno LMS
- Data theft
- System disruption
- Unauthorized access to sensitive information

Affected Versions:

- **opigno_group_manager** < 3.1.1
- **opigno_module** < 3.1.2
- **opigno_learning_path** < 3.1.2

Fixed Versions:

- **opigno_group_manager:** 3.1.1 for Drupal 10.x
- **opigno_module:** 3.1.2
- **opigno_learning_path:** 3.1.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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-2024-029
- https://www.drupal.org/sa-contrib-2024-028
- https://www.drupal.org/sa-contrib-2024-027