August 22, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Drupal published security advisories to address vulnerabilities in the following products:

- Opigno module – versions prior to 7.x-1.23
- Opigno TinCan Question Type module – versions prior to 7.x-1.3

Technical Details

The Opigno module is related to Opigno LMS distribution. Opigno Scorm submodule exposes an API for extracting and handling SCORM packages.

Uploaded files were not sufficiently validated to prevent arbitrary file uploads, which could lead to Remote Code Execution (RCE) and/or Cross Site Scripting (XSS).

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- SA-CONTRIB-2024-032 SA-CONTRIB-2024-031 SA-CONTRIB-2024-030
- Opigno - Critical - Arbitrary PHP code execution - SA-CONTRIB-2024-032
- Opigno TinCan Question Type - Critical - Arbitrary PHP code execution - SA-CONTRIB-2024-031
- Drupal Security Advisories