August 9, 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 of a vulnerability. The vulnerability affects Opigno Learning Path and Opigno module versions prior to 3.1.2 and Opigno group manager prior to 3.1.1.

Technical Details

Opigno Learning path administrative forms allow uploading malicious files which may contain arbitrary code (RCE) or cross site scripting (XSS). These forms were not adequately controlled with permissions that communicate the severity of the permission.

An attacker must have a role with the permission "Manage group content in any group".

The Opigno module is related to Opigno LMS distribution. It implements the module entity, that is a sub-part of a training.

In the opigno_module module, 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).

The attacker have a role with the permission "create opigno tincan activities".

The Opigno group manager project is related to Opigno LMS distribution. It allows to build the contents of learning paths, by combining together modules, courses, and other activities, ordering them, and defining conditional rules for the transitions from one step to the next one.

An administration form allows execution of arbitrary code.

The attacker have the permission "update group learning_path". Additionally, it requires several steps and depends on other data in the system to be in place.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- Opigno Learning path - Critical - Arbitrary PHP code execution - SA-CONTRIB-2024-029
- Opigno module - Critical - Arbitrary PHP code execution - SA-CONTRIB-2024-028
- Opigno group manager - Critical - Arbitrary PHP code execution - SA-CONTRIB-2024-027
- VRM Vulnerability Reports