LOW

CV_2025_06_3: Stored Cross-Site Scripting Vulnerability

AdvisoryID: CV_2025_06_3

Severity: Low

Issued: 2025-06-06

Updated: 2025-10-14

Summary

A specific section of the application stores user input directly in a web page and displays it to other users, which raised concerns about a possible Cross-Site Scripting (XSS) attack. Proper management of this functionality ensures a secure and seamless user experience.

Although the user input is not validated in the report creation, these scripts are not executed when the report is run by end users. The script is executed when the report is modified through the report builder by a user with edit permissions.

CVSS Score: 1.8

Commvault Software

The following versions are impacted. Versions that are not listed are either out of support or unaffected. To view version support lifecyle, see Platform Release Schedule and Lifecycles.

Product	Platforms	Affected Versions	Resolved Version	Status
Commvault	Windows	11.36.0 - 11.36.68	11.40.1	Resolved
Commvault	Linux, Windows	11.32.0 - 11.32.112	11.40.1	Resolved

Resolution

This issue affects older versions of the software and has been resolved in version 11.40 and later.

Acknowledgements

We thank NCIA researchers for responsibly disclosing this issue.