June 27, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Fortra published a security advisory to address a critical vulnerability in the following product:

- Fortra FileCatalyst Workflow – version 5.1.6 Build 135 and prior

Technical Details

A SQL Injection vulnerability in Fortra FileCatalyst Workflow allows an attacker to modify application data. Likely impacts include creation of administrative users and deletion or modification of data in the application database. Data exfiltration via SQL injection is not possible using this vulnerability. Successful unauthenticated exploitation requires a Workflow system with anonymous access enabled, otherwise an authenticated user is required. This issue affects all versions of FileCatalyst Workflow from 5.1.6 Build 135 and earlier.

This vulnerability is rated as a **CRITICAL** 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

- CVE-2024-5276
- Fortra Security Advisories - FI-2024-008
- Fortra Security Advisories