مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# Critical Vulnerability in Fortra FileCatalyst Workflow

Tracking #:432315994

Date:28-06-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability has been identified in Fortra FileCatalyst Workflow, a software solution for file transfer automation.

## TECHNICAL DETAILS:

A critical security vulnerability (CVE-2024-5276) has been identified in Fortra FileCatalyst Workflow, a software solution for file transfer automation. This vulnerability is an SQL injection, which could allow an attacker to modify or steal data from the application database.

**Vulnerability Details:**

- **CVE-2024-5276**:CVSS Score:9.8 Critical: SQL injection vulnerability allowing unauthorized modification of application data (create users, delete/modify data). Data exfiltration is not possible with this specific vulnerability. An attacker can potentially exploit this vulnerability if they can inject malicious SQL code into a vulnerable input field. The likelihood of exploitation depends on whether anonymous access is enabled on the Workflow system. Unauthenticated attacks are possible if anonymous access is enabled, while authenticated attacks are possible regardless. . A proof-of-concept exploit by Tenable demonstrated the vulnerability, logging in anonymously and creating a new admin user. While there have been no active exploitation reports, the release of the exploit raises the risk of imminent attacks

**Affected Versions:**

- FileCatalyst Workflow from 5.1.6 Build 135 and earlier

**Fixed Versions:**

- FileCatalyst Workflow users upgrade to 5.1.6 build 139 (or later)

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the fixed versions on as soon as possible.

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.fortra.com/security/advisory/fi-2024-008