CYBER ADVISORY

Fortra FileCatalyst Workflow Vulnerability

(CVE-2024-5276) (Fortra) (SQL injection) (Critical Vulnerability)

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability with a released exploit proof of concept (POC) known as CVE-2024-5276.[1,2] The vulnerability affects all versions of FileCatalyst Workflow from 5.1.6 Build 135 and earlier.[3] Exploitation of the structured query language (SQL) injection vulnerability may allow a remote unauthenticated attacker to create rogue admin users and manipulate data on the application database.[4]

The Cal-CSIC recommends immediately upgrading to FileCatalyst Workflow version 5.1.6 build 139 or newer.

For further information on applying upgrades please refer to [FileCatalyst Workflow 5.1.6](#).

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

CAL-CSIC-202406-006

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Tenable; "Fortra FileCatalyst Workflow Unauthenticated SQLi;" https://www.tenable.com/security/research/tra-2024-25; accessed 26 June 2024
[2] Bleeping Computer; "Exploit for critical Fortra FileCatalyst Workflow SQLi flaw released;" https://www.bleepingcomputer.com/news/security/exploit-for-critical-fortra-filecatalyst-workflow-sqli-flaw-released/; accessed 26 June 2024
[3] Feedly; "CVE-2024-5276" https://feedly.com/cve/CVE-2024-5276; accessed 26 June 2024
[4] Fortra; "SQL Injection Vulnerability in FileCatalyst Workflow 5.1.6 Build 135 (and earlier)" https://www.fortra.com/security/advisory/fi-2024-008; accessed 26 June 2024

TLP:CLEAR