مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Fortra FileCatalyst Workflow

Tracking #:432316189

Date:28-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability, identified as CVE-2024-6633, has been discovered in Fortra's FileCatalyst Workflow, a widely used file transfer and management tool.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-6633-Exposure of Sensitive Information to an Unauthorized Actor**
- CVSS Score **9.8 Critical**
- The default credentials for the setup HSQL database (HSQLDB) for FileCatalyst Workflow are published in a vendor knowledgebase article. Misuse of these credentials could lead to a compromise of confidentiality, integrity, or availability of the software.
- The HSQLDB is only included to facilitate installation, has been deprecated, and is not intended for production use per vendor guides.

Affected Versions:

- FileCatalyst Workflow 5.1.6 Build 139 (and earlier)

Fixed Version:

- FileCatalyst Workflow 5.1.7 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Fortra.

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/advisories/product-security/fi-2024-011