مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in Fortra FileCatalyst Workflow

Tracking #:432315706

Date:18-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Critical RCE Vulnerability in Fortra FileCatalyst Workflow that poses a significant threat to file transfer security.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-25153: 9.8 CRITICAL**
  - A directory traversal vulnerability exists within the ftpservlet component of FileCatalyst Workflow's web portal. Malicious actors can leverage this flaw to upload files to unauthorized locations on the server using specially crafted POST requests.
  - If attackers can upload a file to the web server's root directory, they can execute arbitrary code, potentially installing web shells for persistent remote access.

- **Affected Versions:**
  - All versions of Fortra FileCatalyst Workflow prior to version 5.1.6 Build 114.

- **Fixed Versions:**
  - FileCatalyst 5.1.6 Build 114 or higher.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the security patch released by Fortra 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.