VEILLE Technologique

Vulnérabilité SQLI dans Fortra FileCatalyst

Vulnérabilité SQLI Critique trouvée dans Fortra FileCatalyst Workflow

Qu’est-ce que Fortra FileCtalyst : FileCatalyst Workflow est un portail Web qui permet aux utilisateurs de partager, modifier et suivre des fichiers avec n'importe qui au sein de leur organisation. Dans l'intention expresse de rationaliser vos flux de travail, les zones de fichiers sont délimitées pour que les utilisateurs puissent stocker des fichiers à des fins de traitement et de modification collaborative.

Cette vulnérabilité est associée à la référence CVE-2024-5276, son score CVSS est de 9,8 , ce qui représente un niveau quasiment maximal de sévérité. La vulnérabilité d'injection SQL dans le flux de travail Fortra FileCatalyst pourrait être exploitée par des attaquants distants non authentifiés afin de créer des utilisateurs administrateurs malhonnêtes et de manipuler des données dans la base de données d'applications. Selon Fortra dans un bulletin de sécurité, la faille offre à l'administrateur la possibilité de créer des utilisateurs et de manipuler des bases de données, mais il est impossible de voler des données. Selon le Bulletin de Fortra, il y a une vulnérabilité d'injection SQL dans Fortra FileCatalyst Workflow qui permet à un attaquant de modifier les données de l'application. La création d'utilisateurs administratifs et la suppression ou la modification des données dans la base de données des applications sont des effets probables. Il est impossible d'exfiltrer des données en utilisant cette vulnérabilité pour injecter SQL. Les versions précédentes de FileCatalyst Workflow 5.1.6 Build 135 sont affectées par la faille. Les modifications ont été mises à disposition dans FileCatalyst Workflow 5.1.6 build 139, qui est la version recommandée pour les utilisateurs pour être mise à jour.

Pour conclure Les utilisateurs qui ne peuvent pas appliquer les correctifs immédiatement peuvent désactiver les servlets vulnérables – csv_servlet, pdf_servlet, xml_servlet et json_servlet – dans le fichier "web.xml" situé dans le répertoire d'installation d'Apache Tomcat en tant que solutions de contournement temporaires.

La société de cybersécurité Tenable, qui a signalé la faille le 22 mai 2024, a depuis publié un exploit de preuve de concept (PoC) pour la faille.

Source :

https://www.bleepingcomputer.com/news/security/exploit-for-critical-fortra-filecatalyst-workflow-sqli-flaw-released/

https://www.fortra.com/fr/lignes-de-produit/filecatalyst

https://thehackernews.com/2024/06/critical-sqli-vulnerability-found-in.html