Fortra ha solucionado una grave vulnerabilidad de seguridad que afecta a FileCatalyst Workflow, la cual podría ser explotada por un atacante remoto para obtener acceso administrativo.

La vulnerabilidad, identificada como CVE-2024-6633, tiene una puntuación CVSS de 9.8 y se debe al uso de una contraseña estática para conectar con una base de datos HSQL.

> *«Las credenciales por defecto para la configuración de la base de datos HSQL (HSQLDB) de FileCatalyst Workflow están publicadas en un artículo de la base de conocimientos del proveedor. El mal uso de estas credenciales podría comprometer la confidencialidad, integridad o disponibilidad del software»,* explicó Fortra en un aviso.
>
> *«El HSQLDB solo se incluye para facilitar la instalación, ha sido retirado y no está destinado para su uso en producción según las guías del proveedor. Sin embargo, los usuarios que no hayan configurado FileCatalyst Workflow para usar una base de datos alternativa según las recomendaciones son vulnerables a ataques de cualquier fuente que pueda acceder al HSQLDB.»*

La empresa de ciberseguridad Tenable, que ha sido acreditada por descubrir y reportar la vulnerabilidad, señaló que el HSQLDB es accesible remotamente en el puerto TCP 4406 de manera predeterminada, permitiendo a un atacante remoto conectarse a la base de datos usando la contraseña estática y realizar operaciones maliciosas.

Después de una divulgación responsable el 2 de julio de 2024, Fortra lanzó un parche para corregir el problema de seguridad en FileCatalyst Workflow 5.1.7 o versiones posteriores.

> *«Por ejemplo, el atacante podría agregar un usuario con nivel administrativo en la tabla DOCTERA_USERS, permitiendo el acceso a la aplicación web Workflow como*

> *un usuario administrador»,* explicó Tenable.

Además, la versión 5.1.7 también abordó una vulnerabilidad de inyección SQL de alta gravedad (CVE-2024-6632, puntuación CVSS: 7.2) que explota un paso de envío de formularios durante el proceso de configuración para realizar modificaciones no autorizadas en la base de datos.

> *«Durante el proceso de configuración de FileCatalyst Workflow, se solicita al usuario que proporcione información de la empresa a través de un formulario»*, señaló Robin Wyss, investigador de Dynatrace.
>
> *«Los datos ingresados se utilizan en una consulta de la base de datos, pero la entrada del usuario no pasa por una validación adecuada. Como resultado, el atacante puede modificar la consulta. Esto permite realizar cambios no autorizados en la base de datos.»*