Se ha descubierto una falla de seguridad crítica en Fortra FileCatalyst Workflow que, si no se corrige, podría permitir a un atacante alterar la base de datos de la aplicación.

Registrada como CVE-2024-5276, la vulnerabilidad tiene una puntuación CVSS de 9.8. Afecta a las versiones de FileCatalyst Workflow 5.1.6 Build 135 y anteriores. Se ha solucionado en la versión 5.1.6 Build 139.

> *«Una vulnerabilidad de inyección SQL en Fortra FileCatalyst Workflow permite a un atacante modificar los datos de la aplicación. Los impactos probables incluyen la creación de usuarios administrativos y la eliminación o modificación de datos en la base de datos de la aplicación»,* dijo Fortra en un aviso publicado el martes.

También se destacó que una explotación exitosa sin autenticación requiere un sistema Workflow con acceso anónimo habilitado. Alternativamente, también puede ser explotada por un usuario autenticado.

Los usuarios que no puedan aplicar los parches de inmediato pueden deshabilitar los servlets vulnerables – csv_servlet, pdf_servlet, xml_servlet y json_servlet – en el archivo «web.xml» ubicado en el directorio de instalación de Apache Tomcat como medidas temporales.

La empresa de ciberseguridad Tenable, que reportó la vulnerabilidad el 22 de mayo de 2024, ha lanzado desde entonces un exploit de prueba de concepto (PoC) para la vulnerabilidad.

> *«Un jobID proporcionado por el usuario se usa para formar la cláusula WHERE en una consulta SQL. Un atacante remoto anónimo puede realizar una inyección SQL a través del parámetro JOBID en varios puntos finales URL de la aplicación web del workflow»,* dijo.