Una vulnerabilidad de día cero que afecta a la aplicación de transferencia de archivos administrada GoAnywhere MFT de Fortra, está siendo explotada activamente en la naturaleza.

Los detalles de la vulnerabilidad fueron compartidos públicamente por primera vez por el reportero de seguridad Brian Krebs en Mastodon. Fortra no ha publicado ningún aviso.

La vulnerabilidad es un caso de inyección remota de código que requiere acceso a la consola administrativa de la aplicación, por lo que es imperativo que los sistemas no estén expuestos a la Internet pública.

Según el investigador de seguridad Kevin Beaumont, hay más de 1000 instancias locales a las que se puede acceder públicamente a través de Internet, la mayoría de las cuales se encuentran en Estados Unidos.

> *«El aviso de Fortra citado por Krebs aconseja a los clientes de Anywhere MFT que revisen a todos los usuarios administrativos y controles los nombres de usuario no reconocidos, especialmente los creados por el sistema»*, dijo Caitlin Condon, investigadora de Rapid7.

> *«La deducción lógica es que es probable que Fortra vea un comportamiento de seguimiento del atacante que incluye la creación de nuevos usuarios administrativos u otros para hacerse cargo o mantener la persistencia en los sistemas de destino vulnerables».*

De forma alterna, la compañía de seguridad cibernética dijo que es posible que los hackers exploten las credenciales reutilizadas, débiles o predeterminadas para obtener acceso administrativo a la consola.

Acutalmente no existe un parche disponible para la vulnerabilidad de día cero, aunque Fortra ha lanzado soluciones alternativas para eliminar la configuración del *«servlet de respuesta de licencia»* del archivo web.xml.

Las vulnerabilidades en las soluciones de transferencia de archivos se han convertido en objetivos atractivos para los hackers, con fallas en Accellion y FileZen armadas para el robo de datos y la extorsión.