Investigadores de seguridad cibernética revelaron los detalles de una vulnerabilidad ahora parcheada en el mecanismo de autenticación multifactor (MFA) de Box, que podría abusarse para eludir completamente la verificación de inicio de sesión basada en SMS.

> *«Usando esta técnica, un atacante podría utilizar credenciales robadas para comprometer la cuenta de Box de una organización y filtrar datos confidenciales sin acceso al teléfono de la víctima»,* dijeron los investigadores de Varonis.

La compañía de seguridad dijo que informó el problema al proveedor de servicios en la nube el 2 de noviembre de 2021, por lo que Box emitió las correcciones.

MFA es un método de autenticación que se basa en una combinación de factores como una contraseña (algo que solo el usuario conoce) y una contraseña temporal de un solo uso, también conocida como TOTP (algo que solo el usuario tiene) para proporcionar a los usuarios una segunda capa de defensa contra el relleno de credenciales y otros ataques de apropiación de cuentas.

Esta autenticación de dos pasos puede implicar el envío del código como un SMS o, alternativamente, acceder a través de una aplicación de autenticación o una clave de seguridad de hardware. Por lo tanto, cuando un usuario de Box que está inscrito para la verificación por SMS inicia sesión con un nombre de usuario y contraseña válidos, el servicio establece una cookie de sesión y redirige al usuario a una página donde se puede ingresar el TOTP para obtener acceso a la cuenta.

El bypass identificado por Varonis es una consecuencia de lo que los investigadores llamaron una confusión de modos MFS. Ocurre cuando un atacante inicia sesión con las credenciales de la víctima y abandona la autenticación basada en SMS a favor de un proceso diferente que utiliza, por ejemplo, la aplicación de autenticación para completar con éxito el inicio de sesión simplemente proporcionando el TOTP asociado con su propia cuenta de Box.

> *«Box pasa por alto que la víctima no se ha inscrito en una aplicación y, en cambio, acepta ciegamente una contraseña de autenticación válida de una cuenta totalmente diferente sin verificar primero que pertenecía al usuario que estaba iniciando sesión. Esto hizo posible acceder a la cuenta de Box de la víctima sin acceder a su teléfono o notificar al usuario por SMS»,* dijeron los investigadores.

Además de que Box no verificó si la víctima estaba inscrita en una verificación basada en una aplicación de autenticación (o cualquier otro método que impida los SMS), Tampoco validó que el código ingresado sea de una aplicación de autenticación que en realidad está vinculada a la víctima que está intentando iniciar sesión.

Los hallazgos llegan poco más de un mes después de que Varonis revelara una técnica similar que podría permitir a los malos actores eludir la verificación basada en autenticadores *«dando de baja a un usuario de MFA luego de proporcionar un nombre de usuario y una contraseña, pero antes de proporcionar el segundo factor».*

> *«El punto final /mfa/unenrollment no requería que el usuario estuviera completamente autenticado para eliminar un dispositivo TOTP de la cuenta de un usuario»,* dijeron los investigadores a inicios de diciembre de 2021.

> *«MFA es tan bueno como el desarrollador que escribe el código y puede proporcionar una falsa sensación de seguridad. El hecho de que MFA esté habilitado no significa necesariamente que un atacante deba obtener acceso físico al dispositivo de una víctima para comprometer su cuenta».*