Zoom ha existido por nueve años, sin embargo, su popularidad ha aumentado considerablemente debido a su facilidad de uso durante la pandemia por el coronavirus.

Aunque Zoom es una solución muy eficiente para reuniones de videollamada en línea, no es la mejor opción cuando se habla de privacidad y seguridad.

Según el último hallazgo del experto en seguridad cibernética @_g0dmode, que también fue confirmado por el investigador Matthew Hickey y Mohamed A. Baset, el cliente Zoom para Windows es vulnerable a *«inyección de ruta UNC»*, que podría permitir a los atacantes remotos robar credenciales de inicio de sesión para las víctimas que utilizan sistemas Windows.

El ataque involucra la técnica SMBRelay, en la que Windows expone automáticamente el nombre de usuario de inicio de sesión del usuario y los hash de contraseña NTLM a un servidor SMB remoto cuando intenta conectarse y descargar un archivo alojado en él.

Sin embargo, el ataque solo es posible en Zoom para Windows porque admite rutas remotas UNC, que convierte esas URL potencialmente inseguras en hipervínculos para destinatarios en un chat personal o grupal.

Para robar la credencial de inicio de sesión del usuario que ejecuta Zoom para Windows, todo lo que un atacante debe hacer es enviar una URL diseñada (por ejemplo, \xxxx\abc_file) a la víctima por medio de su interfaz de chat, como se muestra, y esperar a que la víctima haga clic en ella.

Cabe mencionar que las contraseñas capturadas no son texto sin formato, pero una débil se puede descifrar fácilmente en segundos utilizando herramientas para descifrar contraseñas como HashCat o John the Ripper.

En un entorno compartido, como el espacio de oficina, los detalles de inicio de sesión robados se pueden reutilizar de inmediato para comprometer a otros usuarios o recursos de TI y lanzar nuevos ataques.

Además de robar las credenciales de Windows, la falla también se puede aprovechar para lanzar cualquier programa que ya esté presente en una computadora específica o que se descargue como parte de la campaña de ingeniería social del atacante.

Zoom ya fue notificado sobre el error, pero debido a que la falla aún no se ha parcheado, se recomienda a los usuarios que utilicen el software de videoconferencia alternativo o Zoom en su navegador web en lugar de la aplicación cliente dedicada.

Además de utilizar siempre una contraseña segura, los usuarios de Windows también pueden cambiar la configuración de la política de seguridad para restringir que el sistema operativo pase de forma automática sus credenciales NTML a un servidor remoto.

Ayer otro informe confirmó que Zoom no utiliza el cifrado de extremo a extremo para proteger los datos de llamadas de sus usuarios de miradas indiscretas a pesar de decirles a los usuarios que *«Zoom está utilizando una conexión cifrada de extremo a extremo».*

La semana pasada, Zoom actualizó su aplicación para iOS luego de que descubrió que compartía la información del dispositivo de los usuarios con los servidores de Facebook, lo que generó preocupación por su falta de interés en la protección de la privacidad de los usuarios.

A inicios del 2020, Zoom también corrigió otro error de privacidad en su software que podría haber permitido que personas no invitadas se unan a reuniones privadas y espíen de forma remota el audio, el video y los documentos privados compartidos durante la sesión.