Zoom solucionó recientemente una nueva falla de seguridad que podría haber permitido a los hackers potenciales descifrar el código de acceso numérico utilizado para asegurar reuniones privadas en la plataforma y espiar a los participantes.

Las reuniones de Zoom están protegidas por defecto con una contraseña numérica de seis dígitos, pero según Tom Anthony, vicepresidente de productos de SearchPilot que identificó el problema, la falta de limitación de velocidad permitió que *«un atacante intentara todas las un millón de contraseñas en cuestión de minutos y obtener acceso a las reuniones de Zoom privadas de otras personas».*

Cabe señalar que Zoom comenzó a requerir un código de acceso para todas las reuniones en abril, como medida preventiva para combatir los ataques de bombardeo con Zoom, que se refiere al hecho de interrumpir y secuestrar reuniones de Zoom sin invitación para compartir contenido inadecuado.

Anthony informó el problema de seguridad a la compañía el 1 de abril de 2020, junto con un script de prueba de concepto basado en Python, una semana después de que Zoom solucionó el problema el 9 de abril.

El hecho de que las reuniones estaban, de forma predeterminada, aseguradas por un código de seis dígitos, significaba que solo podría haber un máximo de un millón de contraseñas.

Pero con la ausencia de comprobaciones para intentos repetidos de contraseña incorrecta, un atacante puede aprovechar el cliente web de Zoom para enviar continuamente solicitudes HTTP para probar todas las combinaciones.

> *«Con una mejora en el subprocesamiento y la distribución a través de 4-5 servidores en la nube, podría verificar todo el espacio de la contraseña en unos minutos»,* dijo Anthony.

El ataque funcionó con reuniones recurrentes, lo que implica que los hackers podrían haber

tenido acceso a las reuniones en curso una vez que se descifró el código de acceso.

El investigador también descubrió que el mismo procedimiento podría repetirse incluso con reuniones programadas, que tienen la opción de anular el código de acceso predeterminado con una variante alfanumérica más larga, y ejecutarlo contra una lista de las 10 millones de contraseñas principales para realizar un inicio de sesión por fuerza bruta.

De forma separada, se descubrió un problema durante el proceso de inicio de sesión utilizando el cliente web, que empleó una redirección temporal para buscar el consentimiento de los clientes a sus términos de servicio y política de privacidad.

> *«Hubo un encabezado CSRF HTTP enviado durante este paso, pero si lo omitió, la solicitud parecía funcionar bien de todos modos. La falla en el token CSRF hizo que sea aún más fácil abusar de lo que sería de otra forma, pero arreglar eso no proporcionaría mucha protección contra el ataque»*, dijo Anthony.

Luego de los hallazgos, Zoom desconectó el cliente web para mitigar los problemas el 2 de abril antes de emitir una solución una semana después.