Zoom, el software de videoconferencia ampliamente utilizado, solucionó una vulnerabilidad que podría haber permitido a cualquier persona espiar de forma remota reuniones activas sin protección, exponiendo potencialmente audio, video y documentos privados compartidos durante la sesión.

Además de organizar reuniones virtuales y seminarios web protegidos con contraseña, Zoom también permite a los usuarios configurar una sesión de participantes no registrados previamente que pueden unirse a una reunión activa ingresando una ID de reunión única, sin requerir una contraseña o pasar por las salas de espera.

Zoom genera dicha ID de reunión aleatoria, compuesta por números de 9, 10 y 11 dígitos, para cada reunión que se programe. Si se filtra más allá de un grupo de personas individual o previsto, el simple hecho de conocer las ID de las reuniones podría permitir que invitados no deseados se unan a reuniones o seminarios web.

Para sortear este tipo de escenarios, Zoom introdujo a finales del año pasado, algunos controles adicionales en la configuración de contraseña para reuniones y seminarios, que según Check Point, fue el resultado de la investigación sobre laguna en la seguridad de la empresa de seguridad de forma responsable reportado a la compañía en julio de 2019.

En un informe los investigadores de Check Point demostraron un ataque de enumeración automatizado pero no sofisticado para identificar reuniones aleatorias válidas en lugar de utilizar la técnica de fuerza bruta.

> *«Un pirata informático podría generar previamente una larga lista de ID de Zoom Meeting, usar técnicas de automatización para verificar rápidamente si una ID de Zoom Meeting respectiva era válida o no, y luego obtener acceso a reuniones de Zoom que no estuvieran protegidas con contraseña»,* dijeron los investigadores.
>
> *«Pudimos predecir 4% de las ID de reunión generadas de forma aleatoria, lo que es una posibilidad muy alta de éxito, en comparación con la fuerza bruta pura»,*

> agregaron.

Como resultado de la divulgación de Check Point, Zoom introdujo las siguientes características y funcionalidades de seguridad en su servicio de videoconferencia basado en la nube:

- Contraseñas predeterminadas Zoom – Ahora, de forma predeterminada, genera automáticamente una contraseña numérica de seis dígitos para cada reunión que cree que los participantes deben ingresar al unirse al ingresar manualmente la ID de la reunión.
- Aplicación de contraseñas de nivel de cuenta y grupo – Bajo nuevos controles, el administrador de la cuenta puede hacer cumplir tres nuevas configuraciones de contraseña en los niveles de cuenta, grupo y usuario.
- Validación de ID de reunión – Zoom ya no indicará de forma automática si una ID de reunión es válida o no válida, lo que dificulta que las secuencias de comandos automáticas determinen reuniones activas. Para cada conexión, la página se cargará e intentará unirse a la reunión. Por lo tanto, un mal actor no podrá reducir rápidamente el grupo de reuniones para intentar unirse.
- Bloqueador de dispositivos – Para evitar ataques de fuerza bruta, los intentos repetidos de escanear en busca de identificadores de reuniones harán que el dispositivo se bloquee por algún tiempo.

En julio del año pasado, Zoom fue noticia luego de una grave vulnerabilidad de seguridad en su aplicación cliente para MacOS, que permitió a hackers remotos o sitios web maliciosos encender la cámara del dispositivo de los usuarios sin su permiso o conocimiento.