Subsecretaría de Defensa

Gobierno de Chile

REF.: Alerta vulnerabilidades aplicación Zoom

SANTIAGO, 04 abril 2020

Referente a alerta y recomendaciones frente a vulnerabilidades de Zoom, les informo lo siguiente:

A.- SITUACIÓN

1. La plataforma Zoom presenta fallo de seguridad en el cliente Windows de zoom.

2. No existen parches para esta vulnerabilidad, la que podría permitir el robo de credenciales, otorgando al atacante privilegios de administrador de Windows. Esto permitiría a través de la manipulación de los links que envía la aplicación Zoom acceder a los distintos recursos del equipo, entre ellos micrófono, cámara, etc.

B.- RECOMENDACIONES

1. NO UTILIZAR Zoom para materias del Servicio ya sea de clasificación pública, reservada o secreta, puesto que información pude ser vulnerada, exponiendo datos de los usuarios y de los servicios, junto a los privilegios de las estaciones de trabajo.

2. Alternativas de herramientas que existe en el mercado para video conferencia, podemos identificar menos vulnerables a las siguientes:
   - Meet de Google, https://gsuite.google.com/intl/es-419/products/meet/
   - Skype de Microsoft, https://www.skype.com/es/

3. Para mayor seguridad, una solución que permite Video Conferencia es implementar Nube Privada a través de NextCloud, que dispone de varias funcionalidades.

4. En caso de tener que utilizar Zoom:
   - Deshabilitar la opción "unirse antes del anfitrión", en su panel de configuración o en los controles del administrador para una llamada, con esto mantendrá un mayor control de los asistentes de la reunión.
   - Deshabilitar la "Transferencia de archivos", minimizando el riesgo de compartir archivos infectados con algún tipo de malware.
   - Impedir la opción de "Permitir que los participantes eliminados se vuelvan a unir" para que la gente que ha sido expulsada del chat no pueda volver a entrar.
   - En caso de tener que usar Zoom, hacerlo en un equipo stand alone y sin información.

5. Mantener las aplicaciones actualizadas permanentemente, siempre directamente sobre la aplicación (en App o Play Store) y no a través de hipervínculos.

C.- OTRAS INFORMACIONES

1. En la última semana, se han publicado más de 1,700 sitios falsos de Zoom, con el propósito de descargar malware o phishing.

2. Ciberdelincuentes usando ataques de fuerza bruta sobre Zoom, han accedido a detalles confidenciales de 2,400 reuniones por día.

3. CSIRT de Gobierno está trabajando en el envío de una alerta y recomendaciones más detalladas, las que serán enviadas prontamente.

Saluda atentamente,

Departamento de Ciberdefensa y Ciberseguridad
Subsecretaría de Defensa