Seguridad Informática: Plataforma Zoom

Recientemente el departamento de Ciberdefensa y Ciberseguridad emitió una alerta frente al uso malicioso que podría estar afectando a los usuarios de Zoom en el sistema operativo Windows.
La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial y existe debido a que el cliente Zoom para Windows procesa automáticamente los comentarios en el chat y convierte las URL con la ruta UNC en enlaces. Un atacante remoto puede engañar a la víctima para que siga este enlace y obtener acceso a las credenciales NTLM, enviadas por el sistema de la víctima.
En resumen, el atacante podría enviar una ruta y persuadir al usuario para que la ejecute, entregándole acceso al protocolo de autenticación de usuarios.
Las versiones afectadas son Zoom para Windows anteriores a 4.6.9 (19253.0401).

Contramedidas sugeridas:

- Mantener siempre actualizado el software a la última versión disponible al día de hoy es Versión: 4.6.9 (19253.0401)

- Establecer toda reunión con contraseña.
- Validar que los participantes sean quienes dicen ser.
- No permitir que se unan usuarios antes que el organizador.
- Otra opción es utilizar Microsoft Teams incluído en la suite de Office 365. (menú inicio del equipo o en https://teams.microsoft.com/)

Si necesitas apoyo para la habilitación favor generar ticket a helpdesk@icscorp.cl

Atentamente
Gustavo Ortiz R.