| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00169-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 02 de abril de 2020 |
| Última revisión | 02 de abril de 2020 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

## RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Zoom referente a una vulnerabilidad que afecta a su producto.

# VULNERABILIDAD

## Impacto

La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial. La vulnerabilidad 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.

## Productos Afectados

Versiones del cliente Zoom para Windows anteriores a 4.6.9 (19253.0401)

## Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

## Enlace

https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
https://www.cybersecurity-help.cz/vdb/SB2020040161

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.02 20:25:59 -03'00'