Precisión sobre publicación en LUN

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT, quiere hacer la siguiente precisión respecto a una publicación realizada por el diario Las Últimas Noticias este martes 7 de abril de 2020.

La publicación titulada *"Por estos motivos el Gobierno aconseja tener más ojo con Zoom"*, sección El Día, página 5, cita el *Informe sobre aplicaciones para videoconferencia* emitido por CSIRT el pasado domingo 5 de abril.

El artículo de prensa señala en su primer párrafo: *"Según el organismo "se han publicado muchas vulnerabilidades sobre esta herramienta" que, a pesar de los esfuerzos de la empresa, subsisten…"*

El informe de CSIRT en su página 6, desde dónde se obtuvo la cita, señala sobre Zoom: **"Es efectivo que se han publicado muchas vulnerabilidades sobre esta herramienta, pero según el historial de nuevas versiones, estas fallas se han solucionado"**

El artículo cita nuevamente el reporte, el que hace mención indirectamente a la vulnerabilidad de tipo UCN path injection, al señalar que *"terceras partes pueden robar las credenciales de login" para acceder a los computadores"*.

Ésta es precisamente una de las vulnerabilidades parchadas el pasado jueves 2 de abril por la plataforma en cuestión, actualización que está disponible en el informe 9VSA20-00165-01 publicado por CSIRT ese mismo día jueves, y que está expresamente indicado en el informe sobre aplicaciones para videoconferencia, en la página 8, y que fue utilizado para el artículo de prensa.

Como CSIRT, creemos que la idea que se puede concluir a partir de la lectura de este artículo de LUN es diferente a la que sostiene nuestro informe.

Más importante aún, el reporte de CSIRT no se limita a informar sobre el uso de esta plataforma de videoconferencia. En su contenido y conclusiones hace mención a otras 7 herramientas, informando sobre el historial de vulnerabilidades e indicando que todas las herramientas han tenido, tienen y tendrán vulnerabilidades, lo que podría afectar su seguridad informática. Lo importante es que, en la medida que el proveedor disponga de las actualizaciones necesarias para solucionar esas vulnerabilidades, los administradores y las personas apliquen los parches de seguridad a la brevedad posible.

CSIRT espera que la precisión aquí compartida permita despejar cualquier duda que pueda surgir al respecto.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.07 12:05:22 -04'00'