ALERTA DE SEGURIDAD CIBERNÉTICA
USO DE VULNERABILIDADES EN ACTIVE DIRECTORY COMO VECTOR DEL RANSOMWARE CONTI EN ATAQUES CON TROYANO EMOTET

El CSIRT de Gobierno insta a los encargados de ciberseguridad del país a implementar los parches publicados por Microsoft para dos vulnerabilidades (CVE-2021-42278 y CVE-2021-42287) dadas a conocer en la actualización mensual de la compañía (conocidas como "Update Tuesday") correspondiente a noviembre de 2021, la cual también fue en su momento publicada por el CSIRT de Gobierno en nuestro sitio web: https://csirt.gob.cl/vulnerabilidades/9vsa21-00519-01/.

Ambas vulnerabilidades permiten el escalamiento de privilegios en Active Directory, y están siendo aprovechadas por ciberdelincuentes en Chile y otros países de Latinoamérica para inyectar el ransomware Conti, usando como vector al troyano Emotet.

Por lo anterior, es clave que no solo ambas vulnerabilidades sean parchadas a la brevedad, sino que el parchado de vulnerabilidades sea realizado regularmente y cuan pronto como sea posible luego de que estas sean dadas a conocer. Por nuestra parte, compartimos regularmente las vulnerabilidades más relevantes en https://www.csirt.gob.cl/vulnerabilidades/.

Color	¿Cuándo se debe usar?	¿Cómo se puede compartir?
TLP: ROJO - No es para divulgación, restringida solo a los participantes.	Se debe utilizar "TLP: ROJO "cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como "TLP: ROJO "con ningún tercero fuera del ámbito donde fue expuesta originalmente. En la mayoría de las circunstancias, TLP:RED debe intercambiarse verbalmente o en persona.
TLP: ÁMBAR - Divulgación limitada, restringida a las organizaciones de participantes.	Se debe utilizar "TLP: AMBAR" cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como "TLP: AMBAR" únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.
TLP: VERDE - Divulgación limitada, restringida a la comunidad.	Se debe utilizar "TLP: VERDE" cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o del sector	Los receptores pueden compartir la información indicada como "TLP: VERDE" con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP: BLANCO - La divulgación no está limitada.	Se debe utilizar "TLP: BLANCO" cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información "TLP: BLANCO" puede ser distribuida sin restricciones, sujeta a controles de Copyright.