Alerta de seguridad cibernética	9VSA20-00290-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de agosto de 2020
Última revisión	24 de agosto 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 obtenida de Wireshark referente a vulnerabilidad que afecta a la disponibilidad de la aplicación. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-17498

Impactos

Es posible para un atacante remoto enviarle datos especialmente diseñados a la aplicación para causar un error de límites en memoria en el disector Kafka.
El envío de paquetes malformados de forma exitosa causaría una condición de denegación de servicios (DoS) en la aplicación.

Productos Afectados

Wireshark desde la versión 3.2.0 hasta la 3.2.5 (incluida).

Mitigaciones

Actualizar Wireshark a la versión 3.2.6.

Enlaces

https://www.wireshark.org/security/wnpa-sec-2020-10.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17498

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.08.24 14:00:32 -04'00'