Alerta de seguridad cibernética	9VSA20-00318-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de noviembre de 2020
Última revisión	05 de noviembre 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 Wireshark respecto a tres vulnerabilidades que podrían causar una denegación del servicio otorgado por Wireshark. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-25862
CVE-2020-25863
CVE-2020-25866

CVE-2020-25866

Es posible hacer fallar al disector BLIP inyectando datos malformados a la red o convenciendo a una víctima para leer un archivo de datos malformados.

Productos Afectados
Wireshark versiones desde la 3.2.0 hasta la 3.2.6, y desde la 3.0.0 hasta la 3.0.13.

Mitigación
Actualizar Wireshark a las versiones 3.2.7, 3.0.14 o posteriores.

Enlaces
https://www.wireshark.org/security/wnpa-sec-2020-13.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25866

CVE-2020-25862

Es posible hacer fallar al disector TCP inyectando datos malformados a la red o convenciendo a una víctima para leer un archivo de datos malformados.

Productos Afectados
Wireshark versiones desde la 3.2.0 hasta la 3.2.6, desde la 3.0.0 hasta la 3.0.13 y desde la 2.6.0 hasta la 2.6.20.

Mitigación
Actualizar Wireshark a las versiones 3.2.7, 3.0.14, 2.6.20 o posteriores.

Enlaces
https://www.wireshark.org/security/wnpa-sec-2020-12.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25862

CVE-2020-25863

Es posible hacer fallar al disector multiparte MIME inyectando datos malformados a la red o convenciendo a una víctima para leer un archivo de datos malformados.

Productos Afectados

Wireshark versiones desde la 3.2.0 hasta la 3.2.6, desde la 3.0.0 hasta la 3.0.13 y desde la 2.6.0 hasta la 2.6.20.

Mitigación

Actualizar Wireshark a las versiones 3.2.7, 3.0.14, 2.6.20 o posteriores.

Enlaces

https://www.wireshark.org/security/wnpa-sec-2020-11.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25863

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.05 14:18:56 -03'00'