Alerta de seguridad informática	9VSA20-00124-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2020
Última revisión	16 de enero 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 información obtenida de Wireshark, referente a vulnerabilidades que afectan a su analizador de paquetes, las cuales de ser explotadas permitirían a un atacante remoto realizar ataques de denegación de servicios sobre los sistemas vulnerables. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2020-7044

CVE-2020-7045

Impacto

Debido a la falta de sanitización de los datos entregados por el usuario en el disector BT ATT, y también, por causa de la corrupción en memoria al inyectar un paquete malformado en la aplicación, es posible para un atacante remoto realizar una denegación de servicios en el sistema afectado.

Productos Afectados

Desde la versión 3.0.0 hasta la 3.0.7.

Mitigación

Actualizar a la versión 3.0.8.

Enlaces

https://www.wireshark.org/security/wnpa-sec-2020-01.html
https://www.wireshark.org/security/wnpa-sec-2020-02.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7045