Alerta de seguridad cibernética	9VSA20-00289-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de agosto de 2020
Última revisión	21 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 Haxx referente a vulnerabilidad que afecta a la confidencialidad de los datos en el proyecto cURL. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-8231

Impactos

Debido a un error de desreferencia de puntero expirado para conexiones "CURLOPT_CONNECT_ONLY", era posible para un atacante enviar datos utilizando la sesión expirada de otro usuario. Esto era posible si el usuario utilizaba "CURLOPT_CONNECT_ONLY" para consultar si un sitio es accesible, de esta forma, el atacante podría forzar a la aplicación a reutilizar la conexión expirada y enviar datos destinados a otra conexión, al servidor controlado por el atacante.

Productos Afectados

Las versiones afectadas son libcurl desde la versión 7.29.0 hasta la 7.71.1 (incluida).

Mitigaciones

Actualizar a la versión 7.72.0 o superior.

Enlaces

https://curl.haxx.se/docs/CVE-2020-8231.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8231