Alerta de seguridad cibernética	9VSA20-00254-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de junio de 2020
Última revisión	26 de junio 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 dos vulnerabilidades que afectan a cURL. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-8169
CVE-2020-8177

CVE-2020-8169

Debido a que cURL envía las consultas DNS con las credenciales proporcionadas para la autenticación HTTP al procesar redirecciones, un atacante remoto que controla un servidor DNS podría obtener acceso a credenciales autenticadas por HTTP.

Productos Afectados
Libcurl desde la versión 7.62.0 hasta la 7.70.0.

Mitigación
Aplicar una de las siguientes medidas:
Actualizar cURL a la versión 7.71.0.
Aplicar el parche en tu versión de libcurl y rebuild.
Desactivar "CURLOPT_FOLLOWLOCATION" o redirigir a HTTP(s).

Enlaces
https://curl.haxx.se/docs/CVE-2020-8169.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8169

CVE-2020-8177

Debido a un error lógico al procesar el encabezado de respuesta HTTP "Content-Disposition:" en cURL, cuando se ejecuta con el indicador -J y los indicadores -i en la misma línea de comando, un atacante remoto podría engañar a una víctima para ejecutar un comando cURL especialmente diseñado contra un sitio web malicioso y sobrescribir archivos en el sistema del usuario.

Productos Afectados
cURL desde la versión 7.20.0 hasta la 7.70.0.

Mitigación
Aplicar una de las siguientes medidas:
Actualizar cURL a la versión 7.71.0.
Aplicar el parche en tu versión de libcurl y rebuild.
No usar -J (en un directorio con archivos pre-existentes).

Enlaces
https://curl.haxx.se/docs/CVE-2020-8177.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8177