

Alerta de seguridad cibernética	9VSA20-00248-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2020
Última revisión	19 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de VideoLan referente a tres vulnerabilidades que afectan a su reproductor de multimedia VLC. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-9308
CVE-2020-13428
CVE-2019-19221

CVE-2020-9308

Debido a las vulnerabilidades encontradas en “libarchive”, es posible causar una denegación de servicios o realizar la ejecución de código remoto en el sistema afectado debido a que “libarchive” intenta descomprimir un archivo mal formado.

Productos Afectados

Afecta a todas las versiones del reproductor VLC.

Mitigación

Actualizar a la versión 3.0.11 ‘Vetinari’ de VLC media player.

Enlaces

<https://github.com/videlalva/vlc-3.0/releases/tag/3.0.11>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9308>

CVE-2020-13428

Debido a un error en memoria en el componente “H26X packetizer”, un atacante remoto podría crear un archivo especialmente diseñado para gatillar el error en memoria y causar una denegación de servicios o posiblemente la ejecución de código remoto con los permisos del usuario afectado. Esta vulnerabilidad solo afecta a macOS/iOS.

Productos Afectados

Afecta a todas las versiones del reproductor VLC para macOS o iOS.

Mitigación

Actualizar a la versión 3.0.11 ‘Vetinari’ de VLC media player.

Enlaces

<https://github.com/videlalva/vlc-3.0/releases/tag/3.0.11>

<https://www.videlalva.org/security/sb-vlc3011.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13428>

CVE-2020-19221

Debido a las vulnerabilidades encontradas en “libarchive”, es posible para un atacante obtener información potencialmente sensible y causar una denegación de servicios a través de la lectura de memoria fuera de los límites establecidos en el sistema afectado, ya que “archive_wstring_append_from_mbs()” no maneja bien la lectura de archivos.

Productos Afectados

Afecta a todas las versiones del reproductor VLC.

Mitigación

Actualizar a la versión 3.0.11 'Vetinari' de VLC media player.

Enlaces

<https://github.com/videlalva/vlc-3.0/releases/tag/3.0.11>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19221>