Alerta de Seguridad Informática (9VSA-00013-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 09 de Julio de 2019

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 Sobre Seguridad Informática, (CSIRT), advierte sobre el software de vídeo conferencias Zoom el cual presenta una vulnerabilidad que permitiría a un atacante tener acceso a la cámara del usuario sin previa autorización.

Vulnerabilidad

CVE-2019–13449

CVE-2019–13450

Impacto

CVE-2019–13449: Una atacante remoto puede provocar una denegación de servicio utilizando una secuencia inválida hacia el cliente Zoom (versiones anteriores a 4.4.2 en macOS)

CVE-2019–13450: En la aplicación Zoom Client y RingCentral para macOS, un atacante remoto puede obligar al usuario a unirse a un video llamado con la cámara activa. Esto ocurre porque cualquier sitio puede interactuar con el servidor web levantado localmente en los puertos 19421 y 19424. Nota: una máquina permanecerá vulnerable aun cuando el cliente haya sido desinstalado.

Productos afectados

Zoom Client

Mitigación

Se recomienda estar atento a las actualizaciones del software.

Si es desinstalada la aplicación se requerirán pasos adicionales para bloquear la explotación, tales como la configuración del parámetro ZDisableVideo y/o eliminar el servidor web borrando el directorio ~/.zoomus y creando un archivo plano ~/.zoomus

Enlace

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13449

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13450

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob