BOLETÍN DE ALERTA

Boletín Número: 2021-04 **Fecha de Publicación:** 22/06/2021

Tema: Múltiples vulnerabilidades en el chipset Jetson de NVIDIA

Importancia: Alta

Resumen:

Se ha reportado a NVIDIA varias vulnerabilidades que afectan a millones de dispositivos de Internet de las cosas (IoT) que ejecutan chips Jetson de NVIDIA abren la puerta a una variedad de ataques, incluidos los ataques de denegación de servicio (DoS) o el desvío de datos.

Clasificados en nueve vulnerabilidades de alta gravedad, incluidos ocho errores adicionales de menor gravedad, recibiendo los siguientes identificadores:

CVE-2021-34372, CVE-2021-34373, CVE-2021-34374, CVE-2021-34375, CVE-2021-34376, CVE-2021-34377, CVE-2021-34378, CVE-2021-34379, CVE-2021-34380.

Recursos Afectados:

- AGX Xavier
- Xavier NX / TX1
- Jetson TX2
- Jetson TX2 NX
- Jetson Nano
- Jetson Nano 2GB

Descripción:

El error más grave, registrado como CVE-2021-34372, abre el marco de Jetson a un ataque de desbordamiento de búfer por parte de un adversario. Según el boletín de seguridad de NVIDIA, el atacante necesitaría acceso de red a un sistema para llevar a cabo un ataque, pero la compañía advirtió que la vulnerabilidad no es compleja de explotar y que un adversario con pocos o bajos derechos de acceso podría lanzarla.

Un ataque podría dar a un adversario acceso persistente a componentes, además del chipset NVIDIA objetivo, y permitir que un pirata informático manipule o sabotee un sistema objetivo según el boletín de seguridad, publicado por NVIDIA.

Otra de las fallas CVE - 2021-34373, con una clasificación de gravedad alta y puntuación de 7,9, afecta el kernel de Linux de confianza de Jetson y abre la puerta a un ataque de desbordamiento de búfer basado en el montón. Este tipo de ataque está dirigido al marco de memoria de

datos del montón del chip, donde el componente se manipula para generar errores.

El kernel de Linux confiable y confiable (TLK) contiene una vulnerabilidad en el kernel de NVIDIA TLK donde la falta de refuerzo del montón podría causar desbordamientos del montón, lo que podría conducir a la divulgación de información y la denegación de servicio.

Además del firmware, el fabricante de chips emitió parches de seguridad para los CVE- 2021-34372 a CVE-2021-34397 para abordar el software de punto final para Jetson TX1, serie TX2, TX2 NX, serie AGX Xavier, Xavier NX, Nano y Nano 2GB.

Riesgos:

- Ataques de denegación de servicio (DoS)
- Desvío de datos
- Escalada de privilegios
- Divulgación de información

Solución:

Para proteger su sistema, descargue e instale los últimos paquetes de actualización de seguridad.

Referencias:

https://nvidia.custhelp.com/app/answers/detail/a_id/5205
https://threatpost.com/nvidia-jetson-chipset-dos-data-theft/167093/
https://calendae.es/errores-en-el-chipset-jetson-de-nvidia-abren-la-puerta-a-ataques-dos-y-robo-de-datos/