Alerta de seguridad informática	**9VSA-00030-001**
Clase de alerta	**Vulnerabilidad**
Tipo de incidente	**Sistema y/o Software Abierto**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**7 de Agosto de 2019**
Última revisión	**7 de Agosto 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 de Seguridad Informática, CSIRT, comparte la información entregada por NVIDIA referente a una actualización para NVIDIA GPU Display Driver, para mitigar 5 vulnerabilidades que pueden permitir ejecución de código local, denegación de servicios o elevación de privilegios.

Vulnerabilidad

- CVE-2019-5683
- CVE-2019-5684
- CVE-2019-5685
- CVE-2019-5686
- CVE-2019-5687

Impacto

CVE-2019-5683

Vulnerabilidad en el componente de registro de trazas del driver de video en modo usuario. Si un atacante tiene acceso al sistema y crea un hard link el software no verifica que sea un ataque hard link. Este comportamiento puede conducir a la ejecución de código, denegación de servicio o escalada de privilegios.

CVE-2019-5684

NVIDIA Windows GPU Display Driver contiene una vulnerabilidad en los controladores DirectX, en la que un shader especialmente diseñado puede causar un acceso fuera de los límites de una matriz de textura de entrada, lo que puede conducir a la denegación del servicio o la ejecución del código.

CVE-2019-5685

NVIDIA Windows GPU Display Driver contiene una vulnerabilidad en los controladores DirectX, en la que un shader especialmente diseñado puede causar un acceso fuera de los límites a una matriz temporal local del shader, lo que puede conducir a la denegación del servicio o la ejecución del código.

CVE-2019-5686

NVIDIA Windows GPU Display Driver contiene una vulnerabilidad en el controlador de capa de modo kernel (nvlddmkm.sys) para DxgkDdiEscape en el que el software utiliza una función API o estructura de datos de una manera que se basa en propiedades que no siempre se garantiza que sean válidas, lo que puede conducir a la denegación de servicio.

CVE-2019-5687

NVIDIA Windows GPU Display Driver contiene una vulnerabilidad en el controlador de capa de modo kernel (nvlddmkm.sys) para DxgkDdiEscapeen el que un uso incorrecto de los permisos predeterminados para un objeto lo expone a un atacante, lo que puede conducir a la divulgación de información o la denegación de servicio.

Productos Afectados

- Driver NVIDIA para Windows
  - GeForce: Versiones R430 anteriores a 431.60
  - Quadro, NVS:
    - Versiones R430 anteriores a 431.70
    - Versiones R418 anteriores a 426,00

- Versiones R400 (actualización disponible la semana de 19 de agosto de 2019)
- Versiones R390 anteriores a 392,56

◦ Tesla: Versiones R418 (actualización disponible la semana de 12 de agosto de 2019)

Mitigación

Instalar las actualizaciones liberadas por el fabricante directamente de su página web.
Importante, para los productos Quadro y NVS la actualización para las versiones vulnerables de la serie R400 estarán disponibles la semana del 19 de agosto del 2019, en cuanto para el producto Tesla la actualización para las versiones vulnerables de la serie R418 estarán disponibles la semana del 12 de agosto del 2019, según lo publicado por el fabricante.

Enlace

https://nvidia.custhelp.com/app/answers/detail/a_id/4841

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.07 10:16:44 -04'00'