Nro. Alerta:	AL-2024-027	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-nov-2024	**VULNERABILIDAD EN PRODUCTOS NVIDIA**	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Varios (DDoS, Command and Control, entre otros)

Nivel de riesgo: Alto

II. ALERTA

Los recientes drivers GeForce Driver 566.03 WHQL de NVIDIA, lanzados el 22 de octubre, pasaron un poco desapercibidos en cuanto a novedades, ya que se centraron en algunas mejoras para juegos y corrección de errores menores. Sin embargo, lo realmente importante ha llegado después: NVIDIA ha completado su boletín de seguridad, y el diagnóstico es más alarmante de lo esperado. Este boletín revela un total de 8 vulnerabilidades, 5 de ellas consideradas críticas con una puntuación CVSS de 8,8 sobre 10.

Figura 1.- *Ilustración asociada a Nvidia* ***Fuente: Gizmodo***

III. INTRODUCCIÓN

NVIDIA ha clasificado estas cinco vulnerabilidades como críticas debido al alto riesgo que suponen. Afectan directamente al kernel del driver y pueden permitir que un atacante ejecute código, provoque una denegación de servicio o escale privilegios en el sistema. A continuación, se detallan cada una de estas vulnerabilidades y sus implicaciones:

- CVE-2019-5665: Una falla en el componente 3D Vision para Windows donde el servicio estéreo abre archivos sin verificar enlaces físicos, lo que podría llevar a la ejecución de código o a la denegación de servicio.
- CVE-2019-5666: Vulnerabilidad en el archivo nvlddmkm.sys dentro del modo kernel que permite la manipulación indebida de índices de matriz, derivando en fallos de seguridad como la denegación de servicio.
- CVE-2019-5667: Otra vulnerabilidad en el modo kernel que, al no gestionar correctamente punteros nulos, puede provocar una ejecución de código o denegación de servicio.
- CVE-2019-5668: Esta vulnerabilidad afecta al comando DxgkDdiSubmitCommandVirtual, con consecuencias similares a las anteriores al desreferenciar punteros nulos.
- CVE-2019-5669: Afecta al DxgkDdiEscape, donde un error de longitud en el búfer puede derivar en accesos fuera de límite, posibilitando así ataques de escalada de privilegios.

IV. VECTOR DE ATAQUE.

En este caso, la compañía ha indicado que si un atacante lograse explotar con éxito estos fallos de seguridad, no tendría un impacto bajo, sino que podría llegar a tener control total sobre el sistema, ya que permitiría realizar un escalado de privilegios, es decir, que el ciberdelincuente podría terminar teniendo los permisos de administrador del sistema.

NVIDIA GPU Display Driver para Windows y Linux contiene una vulnerabilidad que podría permitir a un atacante ejecutar un exploit exitoso de esta vulnerabilidad lo que podría conducir a la ejecución de código, denegación de servicio, escalada de privilegios, divulgación de información y manipulación de datos.

La compañía recomienda a los usuarios que utilicen el sistema operativo Windows y que utilicen GPU GeForce, RTX, Quadro y NVS, actualizar a los controladores 566.03/553.24/538.95, mientras que para quienes utilizan Linux, la marca indica que sería necesario que los actualizasen a la versión 565.57.01/550.127.05/535.216.01 en caso de tener una tarjeta gráfica de cualquier familia de la compañía.

V. INDICADORES DE COMPROMISO

- Si se dispone de una **tarjeta gráfica NVIDIA** y no se actualizado los controladores podría estar en peligro. El fabricante alertó sobre una serie de vulnerabilidades de alta gravedad que permitirían a un atacante ejecutar código, escalar privilegios o manipular tus datos. Los fallos de seguridad no solo afectan a la serie GeForce, sino también a las tarjetas Quadro, Tesla, NVS y otras líneas de producto.

- La empresa ofrece información sobre nuevas vulnerabilidades descubiertas en su software. Todas ellas están catalogadas como graves y afectan a los controladores de sus tarjetas gráficas en Windows y Linux**,** permitiendo que un atacante pueda escalar privilegios para acceder a tu ordenador. Si bien NVIDIA no confirmó si alguna de estas vulnerabilidades ya está siendo explotada, los usuarios deberían actuar pronto.

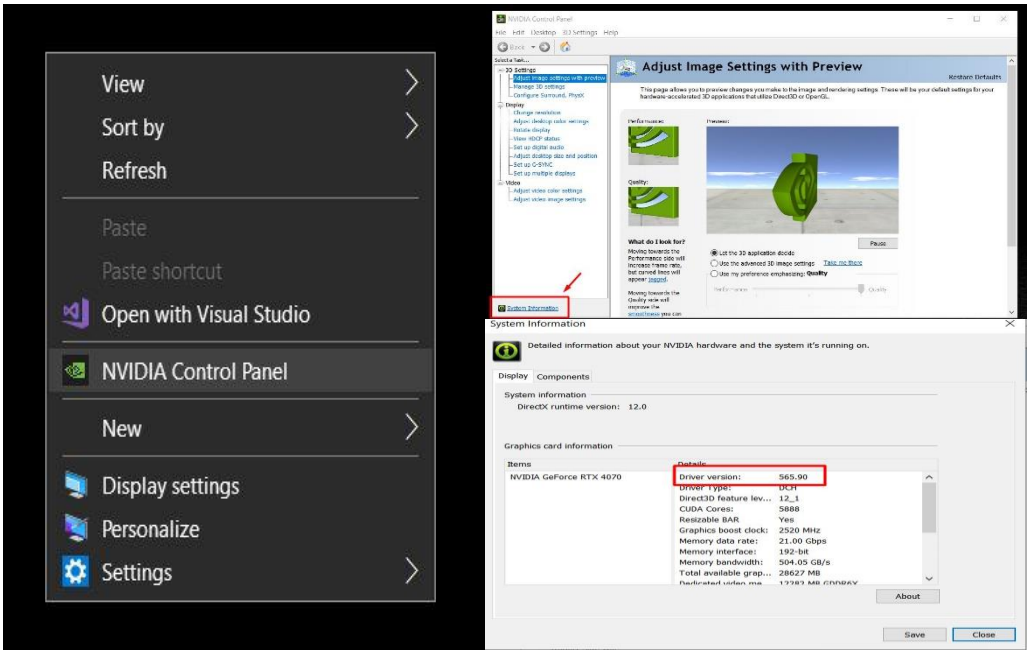
- Una de ellas se aprovecha de un fallo en la validación de entrada para introducir valores inesperados que podrían provocar pantallas azules y consumo excesivo del CPU o RAM**.** Si el atacante consigue controlar las referencias de recursos, tendría acceso a tu información confidencial. También podría valerse de entradas maliciosas para modificar datos o alterar el flujo de control.

- Los agujeros de seguridad no solo están presentes en los controladores de tarjetas gráficas para Windows y Linux. NVIDIA confirmó dos vulnerabilidades en el software de su plataforma de virtualización (vGPU), una de ellas capaz de provocar una validación de entrada incorrecta al comprometer el kernel del sistema operativo.

VI. IMPACTO:

De acuerdo con el boletín de seguridad, todos los usuarios de GeForce que tengan instalada una versión del controlador inferior a la 566.03 son vulnerables. Lo ideal sería actualizar los drivers desde la web de NVIDIA o a través de GeForce Experience, puesto que la última versión corrige los fallos de seguridad e impide que un hacker los aproveche.

Para conocer la versión del controlador de pantalla se debe hacer clic derecho en el escritorio y seleccionar el Panel de Control de NVIDIA**.** Una vez abierto, clic en la opción Información de Sistema, que se encuentra en la esquina inferior izquierda. La versión del controlador instalado aparecerá hasta arriba en la sección de Detalles**.**



Es importante mencionar que si se utiliza la versión Studio de los controladores de pantalla, actualizar el driver no resuelve las vulnerabilidades. NVIDIA no suele liberar las actualizaciones de Gaming y Studio al mismo tiempo, ya que la segunda está enfocada a usuarios profesionales que requieren estabilidad. En este caso, deberá esperar algunos días con la versión actual (565.90).

VII. RECOMENDACIONES:

- Aplicar lo antes posible las actualizaciones mencionadas para mitigar los riesgos potenciales.
- Monitorear los sistemas para detectar cualquier actividad sospechosa posterior a la actualización.
- Evaluar regularmente la seguridad de todos los dispositivos NVIDIA para asegurar que estén protegidos contra futuras vulnerabilidades.
- Los usuarios pueden actualizar los drivers de sus GPU con un puñado de clicks. Generalmente, los PC modernos tienen un **software propio de NVIDIA** que ofrece las versiones más recientes de sus productos. Pero, si este programa no está instalado en tu ordenador, siempre puedes **buscar los drivers manualmente** en la web oficial de NVIDIA.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://es.gizmodo.com/vulnerabilidades-criticas-en-los-ultimos-drivers-de-nvidia-por-que-deberias-actualizar-sin-falta-2000133765

https://hardzone.es/noticias/tarjetas-graficas/vulnerabilidades-drivers-nvidia/

https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidades-en-nvidia-container-toolkit/

https://elchapuzasinformatico.com/2024/10/vulnerabilidades-software-nvidia-ia-nube-recursos-gpu/

https://vandal.elespanol.com/noticia/1350775516/si-tienes-una-tarjeta-nvidia-actualiza-inmediatamente-hay-importantes-vulnerabilidades-de-seguridad/

https://csirt.telconet.net/comunicacion/noticias-seguridad/nvidia-lanza-actualizaciones-de-seguridad-para-varios-productos/