Nro. Alerta:	EC-2022-21	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-febrero-2022	**Vulnerabilidad en el controlador Win32k.sys**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Alto

II. ALERTA

Vulnerabilidad de Windows permite a un atacante local autenticado; obtener privilegios de administrador a través de una vulnerabilidad en el controlador Win32k.sys

Figura 1. Imagen relacionada a Windows10
Fuente: Microsoft

III. INTRODUCCIÓN

El 12 de enero de 2022, Microsoft publicó las actualizaciones de seguridad correspondientes al mes de enero a través de su página Web; las mismas que buscan mitigar 127 vulnerabilidades, de las cuales 10 son de severidad crítica, 92 importantes, 1 media y 24 sin severidad asignada.

Entre las vulnerabilidades corregidas, se menciona: denegación de servicio, escalada de privilegios, divulgación de información, ejecución remota de código, elusión de medidas de seguridad, suplantación de identidad (spoofing).

Por otro lado; en diferentes sitios WEB existen reportes que, muchos administradores omitieron las actualizaciones de 12 enero de 2022 debido a la cantidad significativa de errores entre las cuales se menciona: reinicios, problemas de VPN L2TP, volúmenes ReFS inaccesibles y problemas de Hyper-V. Ante esta problemática, Microsoft lanzó el 18 de enero de 2022 actualizaciones fuera de banda (OOB)

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-21	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-febrero-2022	**Vulnerabilidad en el controlador Win32k.sys**	Versión 1.0

IV. VECTOR DE ATAQUE: Local

En la lista de actualización del 12 de enero de 2022, Microsoft aseguraba corregir una "Vulnerabilidad de elevación de privilegios Win32k" asignada con CVE-2022-21882; sin embargo, el error sigue latente en versiones de Microsoft 10; ya que actualmente existe un exploit que aprovecha esta vulnerabilidad y permitiría a cualquier persona obtener privilegios de SISTEMA en dispositivos Windows 10 vulnerables.

En este sentido; al tratarse de un vector de ataque local, el componente vulnerable no está vinculado a la pila de red y la ruta del atacante es a través de capacidades de lectura/escritura/ejecución como se menciona a continuación:

1. El atacante puede llamar a la API de GUI relevante en el modo de usuario para hacer la llamada del kernel como: xxxMenuWindowProc, xxxSBWndProc, xxxSwitchWndProc, xxxTooltipWndProc, etc.

2. Estas funciones del kernel activarán una devolución de llamada xxxClientAllocWindowClassExtraBytes.

3. El atacante puede interceptar esta devolución de llamada a través del enlace xxxClientAllocWindowClassExtraBytes en KernelCallbackTable y usar el método NtUserConsoleControl para configurar el indicador ConsoleWindow del objeto tagWND, que modificará el tipo de ventana.

Después de la devolución de llamada final, el sistema no verifica si el tipo de ventana ha cambiado y se hace referencia a datos incorrectos debido a una confusión de tipos. La diferencia antes y después de la modificación de la bandera es que antes de establecer la bandera, el sistema piensa que tagWND.WndExtra guarda un puntero de modo_usuario; una vez que se establece el indicador, el sistema cree que tagWND.WndExtra es el desplazamiento del almacenamiento dinámico del escritorio del kernel, y el atacante puede controlar este desplazamiento y luego causar R&W fuera de los límites.

En el siguiente link se puede observar la respectiva prueba de concepto: https://github.com/KaLendsi/CVE-2022-21882

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-21	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-febrero-2022	**Vulnerabilidad en el controlador Win32k.sys**	Versión 1.0

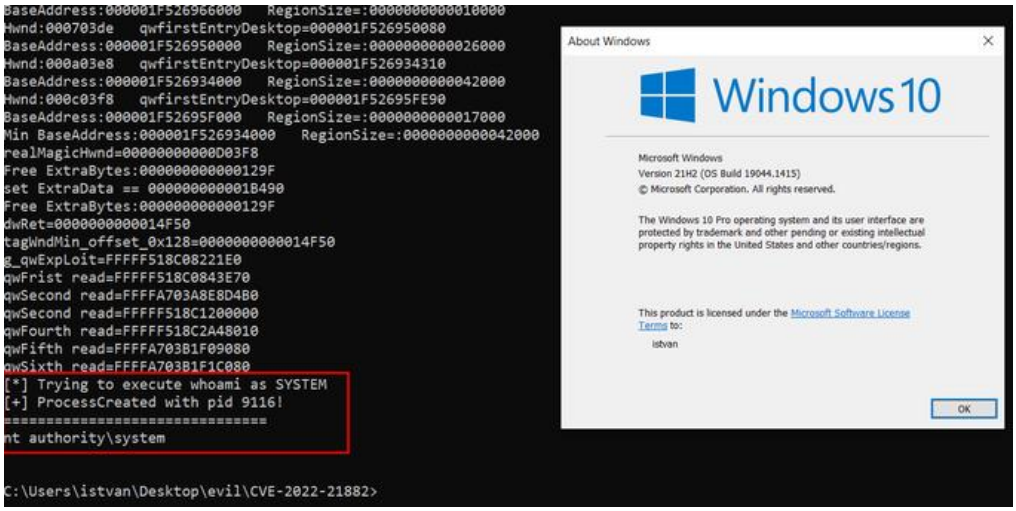

Figura 2. Imagen relacionada a CVE 2022-21882
Fuente: Github.com/tothi

V. IMPACTO:

Existe una pérdida total de confidencialidad originando que todos los recursos dentro del componente afectado se divulguen al atacante; así mismo la integridad como la disponibilidad se ven notablemente afectadas provocando que el atacante pueda denegar completamente el acceso a los recursos en el componente afectado.

Cabe señalar que las versiones afectadas son:

- Versiones de Microsoft Windows 10: 1809, 1909, 20H2, 21H1 y 21H2.
- Microsoft Windows 11.
- Servidor Microsoft Windows 2019.
- Servidor Microsoft Windows 2022.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar actualizaciones de fuentes oficiales.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de información.
- Instalar a la brevedad posible las actualizaciones OOB de Microsoft.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VII. REFERENCIAS:

Abrams, l. (29 de 01 de 2022). *BleepingComputer*. Obtenido de https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/

Helecho, B. (31 de 01 de 2022). *Threatpost*. Obtenido de Threatpost: https://threatpost.com/public-exploit-windows-10-bug/178135/

INCIBE-CERT. (12 de 01 de 2022). *INCIBE-CERT*. Obtenido de INCIBE-CERT: https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/actualizaciones-seguridad-microsoft-enero-2022

Microsoft. (s.f.). *Microsoft*. Obtenido de Microsoft: https://www.microsoft.com/es-ec/d/windows-10-home/d76qx4bznwk4?rtc=1

MICROSOFT, M. (13 de 01 de 2022). *MSRC MICROSOFT*. Obtenido de MSRC MICROSOFT: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882

Team, D. T. (02 de 02 de 2022). *Deepwatch*. Obtenido de Deepwatch: https://www.deepwatch.com/labs/exploit-code-released-for-windows-10-vulnerability/