Identificador
[colCERT AD-0718-008]

18/07/2022

Advertencia de Seguridad Digital

[TLP: WHITE]

Vulnerabilidad Productos Windows (CVE-2022-22047)
Client Service Runtime Process - CSRSS

Contexto

El Client Service Runtime Process – CSRSS, es un proceso legítimo e importante que se ejecutan en el sistema operativo Windows. El archivo csrss.exe auténtico se ubica en "C:\Windows\System32\" y normalmente se ve ejecutándose en el Administrador de tareas.

CSRSS es el encargado de realizar tareas esenciales en el sistema, debido a la gran responsabilidad de sus funciones es clasificado como proceso crítico, algunas de sus servicios son:

- Inicio y finalización de procesos.
- Inicio y finalización de subprocesos.
- Preparación de la ventana de la consola (línea de comandos).
- Desconexión del sistema.

Otros servicios dependen de CSRSS, ya que, si no se ejecuta correctamente, de inmediato dejan de estar disponibles algunas funciones vitales del sistema operativo.

La vulnerabilidad de elevación de privilegios CSRSS de Windows, escala privilegios explotable en el subsistema de tiempo de ejecución de cliente/servidor de Windows (CSRSS) [1].

En la tabla 1 se describe en detalle el producto y el impacto de gravedad al llegarse a explotar esta vulnerabilidad.

Vulnerabilidad	Producto afectado	Descripción	Score
CVE-2022-22047	Windows de anteriores versiones Windows 11 Windows server 2022	Al explotar esta vulnerabilidad, el ciberdelincuente puede obtener privilegios de sistema	7.8

Tabla 1. Detalles de CVE-2022-22047.

En la tabla 2 puede observar no solo el producto y versión afectada sino el parche de mitigación:

Producto	Mitigación
Windows Server 2012 R2 (Server Core installation)	Descargue actualización
Windows Server 2012 R2	Descargue actualización
Windows Server 2012 (Server Core installation)	Descargue actualización
Windows Server 2012	Descargue actualización
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Descargue actualización
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Descargue actualización
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Descargue actualización
Windows Server 2008 for x64-based Systems Service Pack 2	Descargue actualización
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Descargue actualización
Windows Server 2008 for 32-bit Systems Service Pack 2	Descargue actualización
Windows RT 8.1	Descargue actualización
Windows 8.1 for x64-based systems	Descargue actualización
Windows 8.1 for 32-bit systems	Descargue actualización
Windows 7 for x64-based Systems Service Pack 1	Descargue actualización
Windows 7 for 32-bit Systems Service Pack 1	Descargue actualización
Windows Server 2016 (Server Core installation)	Descargue actualización
Windows Server 2016	Descargue actualización
Windows 10 Version 1607 for x64-based Systems	Descargue actualización
Windows 10 Version 1607 for 32-bit Systems	Descargue actualización
Windows 10 for x64-based Systems	Descargue actualización
Windows 10 for 32-bit Systems	Descargue actualización
Windows 10 Version 21H2 for x64-based Systems	Descargue actualización
Windows 10 Version 21H2 for ARM64-based Systems	Descargue actualización
Windows 10 Version 21H2 for 32-bit Systems	Descargue actualización
Windows 11 for ARM64-based Systems	Descargue actualización
Windows 11 for x64-based Systems	Descargue actualización
Windows Server, version 20H2 (Server Core Installation)	Descargue actualización
Windows 10 Version 20H2 for ARM64-based Systems	Descargue actualización
Windows 10 Version 20H2 for 32-bit Systems	Descargue actualización
Windows 10 Version 20H2 for x64-based Systems	Descargue actualización
Windows Server 2022 (Server Core installation)	Descargue actualización
Windows Server 2022	Descargue actualización
Windows 10 Version 21H1 for 32-bit Systems	Descargue actualización
Windows 10 Version 21H1 for ARM64-based Systems	Descargue actualización
Windows 10 Version 21H1 for x64-based Systems	Descargue actualización
Windows Server 2019 (Server Core installation)	Descargue actualización
Windows Server 2019	Descargue actualización
Windows 10 Version 1809 for ARM64-based Systems	Descargue actualización

Windows 10 Version 1809 for x64-based Systems	Descargue actualización
Windows 10 Version 1809 for 32-bit Systems	Descargue actualización

Tabla 2. Actualizaciones en las versiones afectadas.

Algunas de las afectaciones de esta vulnerabilidad:

- Infección de malware adicional ya que existe una elevación de privilegios.
- Exfiltración de identidad: el exploit posee permisos dependiendo del usuario que lo ejecute, si es un administrador, pues tendrá permisos de alto nivel, de esta forma se realiza movimiento lateral para alcanzar un objetivo más grande y así comprometer usuarios en específico o redes en particular.
- Exfiltración de datos sensibles: comprometiendo pilares como confidencialidad, integridad y disponibilidad.

Recomendaciones

- Actualice su sistema operativo a las versiones más recientes tal como se describe en la tabla No. 2.
- Realizar periódicamente la evaluación de la postura de seguridad de los servicios expuestos hacia internet frente a los mecanismos de autenticación para los usuarios.
- Implemente copias de seguridad periódicas y actualizadas de modo que haya disponibilidad sobre la última versión de los datos. Salvaguarde dichas copias de seguridad de modo que no puedan ser modificadas o manipuladas.
- Implemente la segmentación de red, de manera que no se pueda acceder a los equipos de red desde todos los equipos.
- Parchee sistemas operativos, antivirus y programas con las últimas actualizaciones, NO use bajo ningún motivo aplicaciones obsoletas que ya no cuenten con soporte técnico.
- Bloquee los Indicadores de compromiso (IOC) mencionado en esta alerta en sus dispositivos perimetrales.

Referencias

[1] Microsoft, [Online] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22047

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con ColCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT