CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: 20/07/2023

Problemática: Elevación de privilegios del servicio del sistema de eventos SERVICE ICC de Windows

Correlativo: AC-0056

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre la vulnerabilidad identificada como CVE-2023-410133, que afecta al servicio de sistema de eventos SERVICE ICC de Windows.

SITUACIÓN

La vulnerabilidad clasificada como crítica fue encontrada en el servicio de sistema de eventos SERVICE ICC de Windows, que distribuye eventos automáticamente a los componentes del modelo de objetos componentes (COM). El servicio del sistema de eventos SERVICE ICC COM+ de Windows se inicia de forma predeterminada con el sistema operativo y es responsable de proporcionar notificaciones sobre los inicios y cierres de sesión. La explotación exitosa de esta vulnerabilidad permitirá a un atacante elevar los privilegios, ejecutar código arbitrario y realizar ataques de denegación de servicios en sistemas operativos windows.

Los detalles técnicos son desconocidos y un exploit no está disponible públicamente. La técnica de ataque empleada por esta falla es la T1068 según MITRE ATT&CK.

Recursos afectados:

- Microsoft Windows 10 (ver 1809,21H1, 21H2),
- Microsoft Windows 11
- Microsoft Windows Server (ver 2008 R2, 2012 R2, 2022 R2)

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Seguimiento**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alto**

RECOMENDACIONES

Se recomienda a los usuarios de Sistemas Operativos de Microsoft Windows / Server realizar la actualización correspondiente de acuerdo a la versión que corresponda.

- Active las funciones de actualización automática de software en computadoras siempre que sea posible y pragmático.
- Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
- Los clientes que ejecutan una versión afectada de Microsoft Exchange deben habilitar la Protección extendida para estar protegidos contra esta vulnerabilidad

DICCIONARIO DE DATOS

- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
- CVE (Common Vulnerabilities and Exposures); Listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad.
- Atacante (ciberdelincuente): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- DDOs Denial Of Service), es un Dos pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo, y más complicado de detener y determinar su origen.

REFERENCIAS

1. https://msrc.microsoft.com/update-guide/vulnerability
2. https://attack.mitre.org/techniques/T1068/