CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de seguridad

Fecha: 03/01/2023

Problemática: Escalada de Privilegios de Microsoft Windows

Correlativo: AC-0003

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre la vulnerabilidad identificada como CVE-2022-37979, que afecta a los sistemas operativos Windows, Una función desconocida del componente Hyper-V es afectada por esta vulnerabilidad.

SITUACIÓN

La vulnerabilidad clasificada como crítica fue encontrada en Sistemas Operativos Windows. Una función desconocida del componente Hyper-V permite a un atacante aprovechar esta falla y eludir los mecanismos diseñados para controlar los privilegios elevados para obtener permisos de nivel superior. La mayoría de los sistemas modernos contienen mecanismos de control de elevación nativos destinados a limitar los privilegios que un usuario puede realizar en una máquina. Se debe otorgar autorización a usuarios específicos para realizar tareas que pueden considerarse de mayor riesgo. Un adversario puede realizar varios métodos para aprovechar los mecanismos de control integrados a fin de aumentar los privilegios en un sistema.

Los detalles técnicos son desconocidos y un exploit no está disponible públicamente. La técnica de ataque empleada por esta falla es la T1548 según MITRE ATT&CK.

Recursos afectados:

- Microsoft Windows hasta la versión Windows Server 2022

Nivel de priorización

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

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 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.

REFERENCIAS

1. https://msrc.microsoft.com/update-guide/vulnerability
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37979
3. https://nvd.nist.gov/vuln/detail/CVE-2022-37979
4. https://attack.mitre.org/techniques/T1548/