CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: 23/06/2023

Problemática: Vulnerabilidad de divulgación de información de la memoria del kernel de Windows

Correlativo: AC-0047

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre las múltiples vulnerabilidades identificadas como CVE-2022-37996, CVE-2022-37995, CVE-2022-37991, CVE-2022-38039, CVE-2022-37990, CVE-2022-38038, CVE-2022-38037, CVE-2022-37988, CVE-2022-38022, CVE-2022-35761 que afectan a la memoria del kernel de Sistemas Operativos Windows.

SITUACIÓN

un atacante puede llegar a explotar con éxito esta vulnerabilidad, y él tipo de información que podría revelarse es la almacenada en la memoria del kernel, el atacante podría leer el contenido de la memoria desde un proceso en modo usuario. Adicional a este acceso, el ciberdelincuente podría;

- Obtener privilegios de SISTEMA.
- Eliminar carpetas vacías en un sistema vulnerable en el contexto de la cuenta SYSTEM.)No obtendrían privilegios para ver o modificar el contenido de los archivos ni eliminar carpetas que contengan archivos)
- Ejecutar código arbitrario

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
- Código arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
- CVE (Common Vulnerabilities and Exposures); Listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad.
- Ciberlelincuente: 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/CVE-2022-3313
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3311
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3310
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3308
5. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3307
6. https://msrc.microsoft.com/update-guide/vulnerability
7. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3373
8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3370
9. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3317
10. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3316