

Vulnerabilidad de software

Fecha: 01/08/2023

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

Correlativo: AC-0061

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft ha emitido 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.

Nivel de priorización

Prioridad Urgente / No Urgente		Actualización Seguimiento/Preventiva/Resiliente		
Urgente		Preventiva		
Riesgo Alto/ Medio/ Bajo	Integridad	Nivel de Afectación		
		Disponibilidad	Confidencialidad	
Alto	Alto	Alta	Alto	

Matriz de Evaluación

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.
- 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

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3373>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3370>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3317>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3316>

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3313>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3311>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3310>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3308>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3307>