CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de Software

Fecha: 07/11/2022

Problemática: Vulnerabilidad de elevación de privilegios del kernel de Windows.

Correlativo: AA-0071

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft emitió un comunicado para informar a sus usuario sobre la vulnerabilidad identificada como " CVE-2022-37988" que afecta al servicio "Use-After-Free" en sistemas operativos Microsoft Windows. La explotación exitosa de esta vulnerabilidad puede llevar a un atacante a la ejecución de código arbitrario en el sistema objetivo.

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, la vulnerabilidad se encuentra presente en el registro del kernel de Windows cuando hace uso de la función "Use-After-Free" debido al mal manejo de las reasignaciones fallidas bajo presión de memoria.

Recursos Afectados

- Windows,
- Windows Server,
- Windows Server 2019 (Server Core installation),
- Windows 10 Version 21H1 for x64-based Systems,
- Windows 10 Version 21H1 for ARM64-based Systems,
- Windows 10 Version 21H1 for 32-bit Systems,
- Windows Server 2022,
- Windows Server 2022 (Server Core installation),
- Windows 10 Version 20H2 for x64-based Systems,
- Windows 10 Version 20H2 for 32-bit Systems,
- Windows 10 Version 20H2 for ARM64-based Systems,
- Windows 11 for x64-based Systems,
- Windows 11 for ARM64-based Systems,
- Windows 10 Version 21H2 for 32-bit Systems,
- Windows 10 Version 21H2 for ARM64-based Systems,

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	**Alta**	**Alta**	**Alta**

RECOMENDACIONES

- Microsoft recomienda encarecidamente a sus usuarios a realizar la actualización que corresponda para cada producto afectado.
- Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo y filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).
- Código Arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.

REFERENCIAS

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37988
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37988

ÁREA PARA DEFINICIONES