CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad en el controlador del sistema de archivos del CD-ROM de Windows

Fecha: **12/10/2022**

Problemática: **Ejecución remota de código del controlador del sistema de archivos del CD-ROM de Windows**

Correlativo: **AA-0043**

Institución / Sector: **Instituciones Públicas y Privadas**

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**

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre la vulnerabilidad identificada como CVE-2022-38044 que afecta al controlador del sistema de archivos del CD-ROM de Windows.

SITUACIÓN

De acuerdo a la información obtenida a raíz de la investigación realizada por el Centro Estratégico de Monitoreo – CEM, un ciberdelincuente al explotar esta vulnerabilidad podrá ejecutar código arbitrario en el sistema de vulnerado.

Versiones afectadas:

- **Windows 7**
- **Windows 8**
- **Windows 10**
- **Windows 11**
- **Windows server 2008**
- **Windows server 2012**
- **Windows server 2016**
- **Windows server 2019**
- **Windows server 2022**

RECOMENDACIONES

- **Se recomienda a los usuarios de Sistemas Operativos de Microsoft Windows a 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.**

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.**

REFERENCIAS

1. **https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38044https://conciber.gob.gt/?page_id=1208**
2. **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38044**

ÁREA PARA DEFINICIONES

*La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.