CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de seguridad

Fecha: **13/10/2022**

Problemática: **Denegación de servicio del protocolo Internet Key Exchange (IKE)**

Correlativo: **AA-0048**

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

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre la vulnerabilidad identificada como CVE-2022-38036, que afecta al protocolo "Internet Key Exchange (IKE)" de sistemas operativos Microsoft Windows.

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, la vulnerabilidad clasificada como crítica fue encontrada en Sistemas Operativos Windows. Una función desconocida del componente IKE (Internet Key Exchange)Protocol Handler está afectada por esta vulnerabilidad, la manipulación con una entrada desconocida conduce a una denegación de servicio. El programa no libera o libera incorrectamente un recurso antes de que esté disponible para su reutilización. Como impacto, se sabe que afecta la disponibilidad.

Los detalles técnicos son desconocidos y un exploit no está disponible públicamente. La técnica de ataque desplegada por esta falla es T1499 según MITRE ATT&CK.

Recursos afectados:

- **Microsoft Windows 11**
- **Microsoft Exchange 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	**Bajo**	**Alta**	**Bajo**

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**

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.**
- **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.**
- **DDOs: Acrónimo en inglés Denial Of Service (Dos), es un Dos pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo, y más complicado de detener y determinar su origen.**

REFERENCIAS

1. **https://msrc.microsoft.com/update-guide/vulnerability**
2. **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38036**
3. **https://vuldb.com/?id.210511**
4. **https://attack.mitre.org/techniques/T1499/**

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.