CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidades en Microsoft Exchange Server

Fecha: **13/10/2022**

Problemática: **Múltiples vulnerabilidades en el Sistema Operativo Microsoft Exchange Server**

Correlativo: **AA-0045**

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 las múltiples vulnerabilidades identificadas como CVE-2022-41040, CVE-2022-24477, CVE-2022-24516, CVE-2022-21980 que afectan a los Sistemas Operativos Microsoft Exchange Server.

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, para llevar a cabo la explotación exitosa de esta vulnerabilidad, se requiere que el atacante se encuentre autenticado en el servidor de Microsoft Exchange Server o que el usuario con una versión afectada de Exchange Server acceda a un servidor malicioso.

Ambas condiciones conllevarían a que un ciberdelincuente pueda;

- **Ejecutar PowerShell en el contexto del sistema**
- **Ejecutar de forma remota código arbitrario del lado del servidor.**
- **Acceder y apoderarse de los buzones de correo de todos los usuarios de Exchange, por lo que podrá enviar y leer correos electrónicos, así como descargar archivos adjuntos.**
- **Alojar recursos compartidos en un servidor o un sitio web especialmente diseñado.**

RECOMENDACIONES

Se recomienda a los usuarios de Sistemas Operativos de Microsoft Exchange Server 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.**
- **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**
- **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://microsoft.github.io/CSS-Exchange/Security/Extended-Protection/**
2. **https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/**
3. **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040**
4. **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477**
5. **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516**
6. **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980**

ÁREA PARA DEFINICIONES