CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad Microsoft Exchange

Fecha: 30/09/2022

Problemática: Vulnerabilidades criticas de día cero con afectación a Microsoft Exchange Server 2013, 2016 y 2019

Correlativo: AA-0027

Institución / Sector: Gobierno / Sector Privado

CONTEXTO

Por medio de sus canales oficiales Microsoft informó sobre dos vulnerabilidades 0-day, mismos que son ataques dirigidos a servidores Microsoft Exchange en sus versiones 2,013, 2,016 y 2,019, siendo las vulnerabilidades publicadas: CVE-2022-41040 y CVE-2022-41082. Cabe señalar que el acceso autenticado al servidor Exchange vulnerable es necesario para explotar con éxito las descritas con anterioridad.

Microsoft señaló que un atacante necesitaría acceso autenticado al servidor Exchange, por medio del secuestro de credenciales, recientemente publicó parches de seguridad de nivel *crítico* para su implementación inmediata dentro de las configuraciones a nivel de servidor.

SITUACIÓN

Microsoft está investigando dos vulnerabilidades de día cero que afectan a Microsoft Exchange Server 2013, 2016 y 2019. Así mismo la firma de seguridad Trend Micro junto a otras empresas de ciberseguridad otorgan a las vulnerabilidades calificación de gravedad de 8,8 en promedio sobre 10.

En tal sentido se recomienda efectuar de manera inmediata la actualización de parches de seguridad proporcionados por Microsoft, así como un compendio de acciones citadas dentro de este documento en el apartado de recomendaciones.

Nivel de Priorización

Prioridad Urgente / No Urgente	Seguimiento / Preventiva/ Resiliente
Urgente	Preventiva

Matriz de Evaluación

Alto / Medio /Bajo	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alto**	**Alto**

RECOMENDACIONES

1. Aplicar las actualizaciones inmediatamente de las versiones de Microsoft Exchange server 2013, 2016 y 2019.
2. La mitigación actual consiste en agregar una regla de bloqueo de puertos remotos de powershell expuestos, -> Sitio web predeterminado -> Reescritura de URL -> Acciones para bloquear los patrones de ataque conocidos.
3. Ver la guía de mitigaciones en la referencia número (1).

DICCIONARIO DE DATOS

1. Powershell: es una interfaz de consola con posibilidad de escritura y unión de comandos por medio de instrucciones.

REFERENCIAS

4. Guía de referencias mitigaciones cero day https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
5. Informe estado vulnerabilidades cero day https://techcrunch.com/2022/09/30/microsoft-exchange-zero-days/