DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°043**	**Fecha: 19-02-2024**
		Página: 10 de 17

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en Microsoft Exchange Server		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES**:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo elevación de privilegios que afecta a más de 97,000 servidores Microsoft Exchange. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ataques de retransmisión NTLM en Microsoft Exchange Server y escalar privilegios en el sistema. Un ataque exitoso podría permitir a un atacante con permisos elevados en un servidor Exchange acceder a datos confidenciales, como comunicaciones por correo electrónico, y utilizar el servidor para futuros ataques a la red.

2. **DETALLES:**

Microsoft Exchange Server se utiliza ampliamente en entornos empresariales para facilitar la comunicación y la colaboración entre usuarios, proporcionando servicios de correo electrónico, calendario, gestión de contactos y gestión de tareas.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-21410 de tipo de escalada de privilegios de Microsoft Exchange Server, podría permitir a un atacante apuntar a un cliente NTLM como Outlook con una vulnerabilidad de tipo de fuga de credenciales NTLM. Las credenciales filtradas pueden luego transmitirse al servidor Exchange para obtener privilegios como cliente víctima y realizar operaciones en el servidor Exchange en nombre de la víctima. Un atacante que aprovechara con éxito esta vulnerabilidad podría transmitir el hash Net-NTLMv2 filtrado de un usuario a un servidor Exchange vulnerable y autenticarse como usuario.

Por otro lado, el servicio de monitoreo de amenazas “Shadowserver” anunció que sus escáneres han identificado aproximadamente 97,000 servidores vulnerables. Del total de 97,000, el estado vulnerable de aproximadamente 68,500 servidores depende de si los administradores aplicaron mitigaciones, mientras que se confirma que 28.500 son vulnerables a la vulnerabilidad CVE-2024-21410.

Los países más afectados son Alemania (22.903 casos), Estados Unidos (19.434), Reino Unido (3.665), Francia (3.074), Austria (2.987), Rusia (2.771), Canadá (2.554) y Suiza (2.119).

Cabe señalar, que la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) también agregó CVE-2024-21410 a su catálogo de 'Vulnerabilidades explotadas conocidas', dando a las agencias federales hasta el 7 de marzo de 2024 para aplicar las actualizaciones/mitigaciones disponibles o dejar de usar el producto.

A. Productos afectados:

- Múltiples versiones de Microsoft Exchange Server.

3. **RECOMENDACIÓN:**

- Aplicar la actualización acumulativa 14 (CU14) de Exchange Server 2019 publicada durante el martes de parches de febrero de 2024, que habilita las protecciones de retransmisión de credenciales NTLM.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/over-28-500-exchange-servers-vulnerable-to-actively-exploited-bug/ • hxxps://www.cisa.gov/news-events/alerts/2024/02/15/cisa-adds-two-known-exploited-vulnerabilities-catalog