	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°262	Fecha: 02-11-2023
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de día cero en el servidor Microsoft Exchange		
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 día cero (0-Day) de severidad **ALTA** de tipo deserialización de datos que no son de confianza en el servidor Microsoft Exchange. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta**, de tipo deserialización de datos que no son de confianza, existe debido a una validación de entrada insegura al procesar datos serializados dentro de la clase ChainedSerializationBinder. Un usuario remoto puede enviar una solicitud HTTP especialmente diseñada a la aplicación y ejecutar código arbitrario en el sistema de destino.

Esta vulnerabilidad permite a atacantes remotos ejecutar código arbitrario en instalaciones afectadas de Microsoft Exchange. Se requiere autenticación para aprovechar esta vulnerabilidad.

La falla específica existe dentro de la clase ChainedSerializationBinder. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar la deserialización de datos que no son de confianza. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de SYSTEM.

A. Productos afectados:

- Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018.

3. RECOMENDACIONES:

- Restringir la interacción con la aplicación.
- Actualizar el producto afectado cuando el proveedor lance la versión de software que afronte esta vulnerabilidad, pues a la fecha no se conoce ninguna solución oficial.

Fuente de Información:	• hxxp://www.zerodayinitiative.com/advisories/ZDI-23-1578/