	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°289	Fecha: 04-12-2023
		Página: 6 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Servidores Microsoft Exchange vulnerables expuestos a ataques de ejecución remota de código		
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:

La Fundación ShadowServer (The ShadowServer Foundation), indicó, que más de 20,000 mil servidores de correo electrónico de Microsoft Exchange obsoletas en Europa, EE.UU. y Asia expuestos en la Internet pública son vulnerables a múltiples fallas de ejecución remota de código debido a que han alcanzado la etapa de fin de vida útil (EoL). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código en un sistema vulnerable.

2. DETALLES:

Los análisis de Internet de The ShadowServer Foundation muestran que actualmente hay cerca de 20.000 servidores Microsoft Exchange accesibles a través de la Internet pública que han alcanzado la etapa de fin de vida útil (EoL). Los sistemas de correo ejecutan una versión de software que actualmente no tiene soporte y ya no recibe ningún tipo de actualizaciones, siendo vulnerables a múltiples problemas de seguridad, algunos con clasificación de severidad **CRÍTICA**.

Sin embargo, el investigador de seguridad de Macnica, Yutaka Sejiyama, indicó, que descubrió un poco más de 30,000 servidores Microsoft Exchange vulnerables que alcanzaron el fin del soporte. Según los escaneos de Sejiyama en Shodan, a finales de noviembre había 30,635 máquinas en la web pública con una versión no compatible de Microsoft Exchange.

Asimismo, el investigador también comparó la tasa de actualización y observó que, desde abril de este año, el número global de servidores EoL Exchange cayó sólo un 18% desde 43.656, una disminución que calificó como insuficiente.

Sejiyama, indico, que, según los números de compilación obtenidos de los sistemas durante el análisis, hay cerca de 1,800 sistemas Exchange que son vulnerables a las vulnerabilidades ProxyLogon, ProxyShell o ProxyToken.

Por otro lado, la Fundación ShadowServer, indico que algunas de las máquinas que ejecutan versiones anteriores del servidor de correo Exchange son vulnerables a ProxyLogon, un problema de seguridad crítico identificado como CVE-2021-26855, que puede encadenarse con un error menos grave identificado como CVE-2021-27065 para lograr la ejecución remota de código.

A. Productos afectados:

- Servidores de correo electrónico de Microsoft Exchange, versión 2007, 2010 y 2013.

3. RECOMENDACIONES:

- Priorizar la instalación de actualizaciones en los servidores externos, aún a pesar de haber implementado las mitigaciones disponibles en servidores Exchange obsoletos.
- Actualizar a una versión que aún reciba al menos actualizaciones de seguridad, en el caso de las instancias que llegaron al final del soporte.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/over-20-000-vulnerable-microsoft-exchange-servers-exposed-to-attacks/ • hxxps://www.bleepingcomputer.com/news/microsoft/new-microsoft-exchange-zero-days-allow-rce-data-theft-attacks/