	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°236	Fecha: 06-10-2023
		Página: 7 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de ataque dirigido a equipos virtuales en la nube de Azure		
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:

Investigadores de seguridad de Microsoft, han detectado que múltiples actores de amenazas, están intentando vulnerar los entornos en la nube de Azure a través de Microsoft SQL Server vulnerables a la **inyección SQL**. Un ataque exitoso podría permitir a un actor de amenazas obtener acceso a la instancia de SQL Server hospedada en una máquina virtual de Azure con permisos elevados para ejecutar comandos SQL y extraer datos confidenciales.

2. DETALLES:

Los investigadores de seguridad de Microsoft indicaron que esta técnica de movimiento lateral se ha visto anteriormente en ataques a otros servicios como máquinas virtuales y clústeres de Kubernetes. Sin embargo, esta es la primera vez que ven a Microsoft SQL Server ser utilizado para este propósito.
Kubernetes es una plataforma de código abierto para automatizar la implementación, el escalado y la administración de aplicaciones en contenedores.
Microsoft indico, que el vector inicial de los ataques se inicia con la explotación de una vulnerabilidad de tipo inyección SQL en una aplicación en el entorno del objetivo. Esto permite a los actores de amenazas obtener acceso a la instancia de SQL Server hospedada en la máquina virtual de Azure con permisos elevados para ejecutar comandos SQL y extraer datos confidenciales como: bases de datos, nombres de tablas, esquemas, versiones de bases de datos, configuración de red y permisos de lectura/escritura/eliminación.
Si la aplicación comprometida tiene permisos elevados, los atacantes pueden activar el comando "xp_cmdshell" para ejecutar una serie de comandos del sistema operativo (SO) a través de Microsoft SQL, facilitando para ello una shell en el host de la víctima.
El uso de un servicio legítimo para la exfiltración de datos hace que la actividad no parezca sospechosa o genere una alerta por parte de las soluciones de seguridad, lo que permite a los atacantes el robo de información de una manera discreta en el host de la víctima.
Luego, los atacantes intentaron explotar la identidad en la nube de la instancia de SQL Server para acceder al IMDS (servicio de metadatos instantáneos) y obtener la clave de acceso de identidad en la nube. En Azure, a menudo se asignan identidades administradas a los recursos para la autenticación con otros recursos y servicios en la nube. Si los atacantes tienen ese token, pueden usarlo para acceder a cualquier recurso en la nube para el que la identidad tenga permisos.
Microsoft dijo que los atacantes no lograron explotar con éxito esta técnica debido a errores, pero el enfoque sigue siendo válido y constituye una grave amenaza para las organizaciones. Asimismo, indico, que los atacantes eliminaron todos los scripts descargados y borraron las modificaciones temporales de la base de datos para borrar los rastros del ataque.

A. Productos afectados:

- Microsoft SQL Server, múltiples versiones.

3. RECOMENDACIONES:

- Actualizar el producto afectado con la última versión de software disponible que aborda esta vulnerabilidad de tipo inyección SQL.
- Usar **Defender for Cloud** y **Defender for Endpoint** para detectar inyecciones SQL y actividad sospechosa de SQLCMD, ambos empleados en el ataque observado, según lo sugerido por Microsoft.
- Aplicar el principio de privilegios mínimos al conceder permisos de usuario, lo que siempre agrega fricción en los intentos de movimiento lateral.

Fuente de Información:	• hxxps://underc0de.org/foro/noticias-informaticas-120/piratas-informaticos-atacan-las-maquinas-virtuales-en-la-nube-de-azure/