DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 086**	**Fecha: 12-04-2023** **Página 6 de 14**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Se ha descubierto una falla de diseño crítica en Microsoft Azure		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Se ha descubierto una vulnerabilidad crítica por **falla de diseño** en una ruta de explotación que utiliza la autorización de clave compartida de Microsoft Azure, un método de autenticación basado en clave secreta para cuentas de almacenamiento. Con la obtención de esta clave, un atacante podría obtener acceso total a cuentas de almacenamiento y activos comerciales críticos, moverse lateralmente en el entorno y ejecutar código remoto (RCE).

2. **Detalles:**

- El equipo de investigadores de Orca Security, indico que los atacantes podrían explotar una "falla de diseño" descubierta en Microsoft Azure para obtener acceso a las cuentas de almacenamiento, moverse lateralmente en el entorno e incluso ejecutar código remoto.

- ORCA descubrió que es posible abusar y aprovechar las cuentas de almacenamiento de Microsoft mediante la manipulación de las funciones de Azure para robar tokens de acceso de identidades de mayor privilegio, moverse lateralmente, acceder potencialmente a activos comerciales críticos y ejecutar código remoto.
- La ruta de explotación que sustenta este ataque es un mecanismo llamado autorización de clave compartida, que está habilitado de forma predeterminada en las cuentas de almacenamiento.
- Según Microsoft, Azure genera dos claves de acceso a la cuenta de almacenamiento de 512 bits al crear una cuenta de almacenamiento. Estas claves se pueden usar para autorizar el acceso a los datos a través de la autorización de clave compartida o mediante tokens SAS que se firman con la clave compartida.
- Microsoft indico que las claves de acceso a la cuenta de almacenamiento brindan acceso completo a la configuración de una cuenta de almacenamiento, así como a los datos. El acceso a la clave compartida otorga a un usuario acceso completo a la configuración de una cuenta de almacenamiento y sus datos.
- La firma de seguridad en la nube dijo que estos tokens de acceso pueden ser robados mediante la manipulación de **Azure Functions**, lo que podría permitir que un actor de amenazas con acceso a una cuenta con el rol de colaborador de la cuenta de almacenamiento aumente los privilegios y se haga cargo de los sistemas. Específicamente, si se usa una identidad administrada para invocar la aplicación de función, se podría abusar de ella para ejecutar cualquier comando.

- El investigador de Orca, Roi Nisimi, señalo que una vez que un atacante localiza la cuenta de almacenamiento de una aplicación de función a la que se le asigna una identidad administrada sólida, puede ejecutar código en su nombre y, como resultado, adquirir una escalada de privilegios (PE) de suscripción. En otras palabras, al filtrar el token de acceso de la identidad administrada asignada de la aplicación **Azure Functions** a un servidor remoto, un actor de amenazas puede elevar los privilegios, moverse lateralmente, acceder a nuevos recursos y ejecutar un shell inverso en máquinas virtuales.
- Asimismo, el investigador indico que, al anular los archivos de funciones en las cuentas de almacenamiento, un atacante puede robar y exfiltrar una identidad de mayor privilegio y usarla para moverse lateralmente, explotar y comprometer las joyas de la corona más valiosas de las víctimas.

3. Productos afectados:

- Esta vulnerabilidad de falla de diseño afecta a Microsoft Azure.

4. Solución:

- Microsoft recomienda deshabilitar el acceso de clave compartida y usar la autenticación de Azure Active Directory en su lugar. Sin embargo, la autorización de clave compartida todavía está habilitada de forma predeterminada al crear cuentas de almacenamiento.
- En una divulgación coordinada, Microsoft también señalo que "planea actualizar cómo funcionan las herramientas de cliente de Functions con las cuentas de almacenamiento".

Fuentes de información	▪ hxxps://orca.security/resources/blog/azure-shared-key-authorization-exploitation/ ▪ hxxps://learn.microsoft.com/en-us/azure/azure-resource-manager/management/control-plane-and-data-plane ▪ hxxps://msrc.microsoft.com/blog/2023/04/best-practices-regarding-azure-storage-keys-azure-functions-and-azure-role-based-access/