ACTUALIZACIÓN DE ALERTA DE SEGURIDAD DE LA INFORMACIÓN
RANSOMWARE MÁQUINAS EN VIRTUALES IFX
TLP: BLANCO

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior sugiere fuertemente actualizar los productos obsoletos de los componentes Vsphere y abordar todas las vulnerabilidades importantes actuales.

Los encargados de ciberseguridad y el equipo de tecnología deben realizar evaluaciones de sus activos VMware, para procurar que tengan instaladas las últimas versiones compatibles en su infraestructura.

Las instituciones que exponen sus interfaces de administración a internet deberán tomar medidas inmediatas para aumentar los controles de seguridad.

Recomendaciones

- Limitar el acceso a ESXI.
- Utilizar usuarios con privilegios mínimos.
- Minimizar la cantidad de puertos abiertos.
- Utilizar el modo de bloqueo de ESXI, para ser accedido a través de VCenter Server.
- Restringir acceso a través de SSH y a través del SDK.
- Implementar herramientas de seguridad especializadas en servidores tanto para máquinas virtuales y contenedores alojados en el servidor.

Recordar asimismo realizar copias de seguridad regularmente, las que deben ser almacenadas en diferentes lugares y medios, incluyendo una copia fuera de línea o de la institución.

Finalmente, no tenemos evidencia de que la infección se propague a través de correos electrónicos, por lo tanto, no recomendamos bloquear el email entrante de ninguna institución. Por otra parte, sí hacemos un llamado a elevar la seguridad perimetral de su organización.

Ante cualquier inquietud sobre lo mencionado en este documento o las formas de detectar y mitigar la vulnerabilidad analizada, no dude en tomar contacto con el CSIRT a través de su correo electrónico incidentes@interior.gob.cl o su número telefónico corto 1510 (que es equivalente al +56 2 2486 3850).

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.14 14:56:18 -03'00'