CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente Informático

Fecha: 25/09/2023

Problemática: Incidente de seguridad en IFX Networks S.A.S

Correlativo: AC-0072

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

IFX Networks S.A.S., proveedor de servicios tecnológicos del Gobierno de Colombia, fue afectado tras un incidente de seguridad por infección del ransomware «MarioLocker» impactando en la disponibilidad, confidencialidad e integridad de los servicios de más de 50 instituciones públicas y privadas.

SITUACIÓN

Equipo de respuesta a Incidentes de seguridad de la información del Gobierno, emitió el informe correspondiente sobre el comportamiento y perpetración del ataque, concluyendo que el software malicioso polimórfico tiene unas variables de ejecución estrictas para asegurar su funcionamiento en hypervisores ESXI de VMWare.

Tácticas y Tenias utilizada por el adversario según MITRE ATTt&CK TTP´s

TA0002 – Ejecución -T1059 Unix Shell. Crea una Shell de tipo reverse en ESXI -T1064 Scripting. Ejecuta comandos usando el interprete de "esxcli".

TA0005 – Evasión de Defensa -T1027 Ofuscamiento de Archivos e Información. Encripta los datos usando RC4 PRGA. -T1027.005 Remoción de indicadores con herramientas. Contiene cadenas de pila ofuscadas -T1064 Scripting. Ejecuta comandos usando un interprete

TA0007 - Descubrimiento -T1083 Descubrimiento de archivos y directorios. Enumera los Directorios en ESXI. -T1033 Descubrimiento de Usuarios. Identifica los usuarios con privilegios y activos en el sistema.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

RECOMENDACIONES

Ante esta alerta se dan las siguientes recomendaciones para mitigar este tipo de ataques:

- Deshabilite los protocolos de red heredados que pueden usarse para interceptar el tráfico de red
- Asegúrese de que todo el tráfico cableado y/o inalámbrico esté encriptado adecuadamente.
- Utilice las mejores prácticas para los protocolos de autenticación, como Kerberos, y asegúrese de que el tráfico web que pueda contener credenciales esté protegido por SSL/TLS.
- Utilice dispositivos de red y software de seguridad basado en host para bloquear el tráfico de red que no es necesario dentro del entorno
- Limite el acceso a la infraestructura de red y los recursos que se pueden usar para remodelar el tráfico o producir condiciones AiTM.
- Los sistemas de detección y prevención de intrusiones en la red que pueden identificar patrones de tráfico indicativos

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Ciberataque: Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

REFERENCIAS

CSIRT Colombia
https://www.colcert.gov.co/800/articles-280648_Documento_1.pdf