CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente Informático en América del Sur (República del Perú)

Fecha: **06/10/2022**

Problemática: **Sabotaje Informático**

Correlativo: **AA-0031**

Institución / Sector: **Comando Conjunto de las Fuerzas Armadas y El Ejército Nacional del Perú**

CONTEXTO

Comando Conjunto de las Fuerzas Armadas y El Ejército Nacional del Perú recientemente sufrieron un incidente informático que comprometió el correo electrónico de las instituciones. De acuerdo a la información obtenida, el material fue expuesto por el grupo de hackers autodenominado "Guacamaya".

SITUACIÓN

Con base a la investigación realizada por el Centro Estratégico de Monitoreo – CEM, la exfiltración del buzón de correo electrónico se vio expuesto debido a una vulnerabilidad antigua en el cliente de correo electrónico de "Zimbra". Los ciberdelincuentes aprovechándose de esta vulnerabilidad, utilizaron la webshell para descargar todos los correos del store de Zimbra para posteriormente hacerlos públicos en sus plataformas.

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	**Alta**	**Alta**	**Alta**

RECOMENDACIONES

- **Active las funciones de actualización automática de software en computadoras, teléfonos móviles y otros dispositivos conectados siempre que sea posible y pragmático.**
- **Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.**
- **Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos, clientes de correo electrónico y programas ofimáticos.**
- **Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.**
- **Implemente un proceso de gestión de vulnerabilidades basado en riesgos para la infraestructura de TI a fin de identificar y priorizar las vulnerabilidades críticas y las configuraciones incorrectas de seguridad para su corrección.**

Considere implementar:

- **Firewall perimetral**
- **Servicios de Antivirus/Antimalware.**
- **Herramientas de Prevención de Intrusiones en la red (IDS)**
- **Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)**
- **Herramientas de Detección y Respuesta Extendidas (XDR)**

ÁREA PARA DEFINICIONES

REFERENCIAS

1. https://enlacehacktivista.org/index.php?title=Fuerzas_Represivas
2. https://ddosecrets.com/wiki/Distributed_Denial_of_Secrets

DICCIONARIO DE DATOS

1. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
2. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
3. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
4. IDS (Intrusion Detection System): Un sistema de detección de intrusos es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.
5. Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
6. Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.
7. Hacker: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.
8. Zimbra: Programa informático colaborativo que consta de un servicio de correo electrónico.

ÁREA PARA DEFINICIONES