Open TFTP (Trivial File Transfer Protocol)

1. INTRODUCCIÓN

TFTP es un protocolo de transferencia semejante a una versión básica de FTP pero sin autenticación. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una misma red. La conexión se realiza mediante UDP por el puerto 69, aunque se puede utilizar otro puerto. TFTP implementa su propio esquema de confiabilidad mediante UDP, no admite ningún mecanismo de autenticación ni cifrado, por lo que su utilización puede ser un riesgo de seguridad. No se recomienda instalar el cliente de TFTP en los sistemas con acceso a Internet.

TFTP es un protocolo de transferencia de archivos simple, que permite que las aplicaciones de gestión tramiten las configuraciones de los dispositivos de red. Muchos dispositivos de red proporcionan mecanismos mediante los cuales se les puede ordenar que transfieran sus archivos de configuración desde/hacia un servidor TFTP, se han desarrollado varias aplicaciones de gestión que aprovechan estos mecanismos para proporcionar servicios de configuración para gran número de dispositivos de red.

CARACTERÍSTICAS

Algunas características del protocolo TFTP son:

- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia conforme la RFC 1350, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.
- Al utilizar UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto 69 en modo UDP, y cliente a quien se conecta.

2. RIESGO

TFTP fue diseñado para ser una forma muy sencilla de transferir archivos entre máquinas, no posee seguridad, ni mecanismos de control de acceso, no proporciona ningún medio para validar la identidad de una computadora que solicita transferencias de archivos. Dado que TFPT no requiere autenticación, puede ser un proceso relativamente simple para que una máquina se convierta en una computadora admitida en la red, solo debe enviar una solicitud al servidor, y como no hay forma de que TFTP compruebe si la computadora es legítima o no, esta máquina podría convertirse en una máquina admitida en la red.

Cuando TFPT está configurado correctamente, puede garantizar que sólo se puedan transferir los archivos relacionados con bootstrapping (empezar algo sin recursos o con muy pocos recursos), por lo general se restringe a un determinado directorio. Si TFTP no está configurado correctamente y no está restringido a un directorio que sólo contenga archivos para propósitos de arranque, puede ser posible que cualquier máquina utilice TFTP y copie cualquier archivo (/ etc / passwd por ejemplo) en su propia máquina sin ningún tipo de verificación de autenticación y sin verificaciones de permisos de archivos o directorios.

TFTP no tiene qué ser visible en sistemas expuestos a Internet. Sin embargo, existen muchos servidores TFTP abiertos al público. TFTP ofrece un factor de amplificación mayor que otros protocolos de Internet y puede permitir a los atacantes utilizar estos servidores abiertos al público para amplificar su tráfico, de manera similar a otros ataques DDoS de amplificación como la amplificación de DNS, se puede amplificar hasta 60 veces la cantidad de tráfico original (ataque de amplificación). El atacante suplanta la IP de la víctima y envía muchas solicitudes al servidor, la respuesta de TFTP va a ser mayor que la solicitud, quien las recibe va a ser la víctima y no el atacante, la victima recibe inundaciones con tráfico no deseado, ataque DDoS.

3. DETECCIÓN

Una forma común para buscar máquinas con TFTP configurado incorrectamente es realizar transmisiones dirigidas de paquetes de solicitud de TFTP a diferentes redes y ver qué máquinas responden. Para verificar si se tiene TFTP habilitado, se usa el comando siguiente comando:

"tftp [IP] 69"

Cuando se visualiza el prompt tftp, se escribe el siguiente comando:

get [nombre_cualquiera]

Si TFTP se está ejecutando, se ve un código de error en respuesta, puede que se necesite buscar la respuesta utilizando tcpdump, si la respuesta se envía a algún puerto distinto de 69/UDP.

Los mensajes de error que indican que TFTP está habilitado son:

Error	Mensaje
1	File not found
2	Access violation

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Hace referencia al nombre de la vulnerabilidad
Dirección IP	Dirección IP del dispositivo en cuestión
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5

status_EcuCERT	Online: vulnerabilidad reportada por *Stakeholders* y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por *Stakeholders*, pero en el timestamp_EcuCERT no se detectó.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del dispositivo en cuestión
protocol	Protocolo de respuesta (siempre UDP)
port	Puerto del cual vino la respuesta TFTP provino (usualmente 69/UDP, pero la respuesta puede provenir de cualquier puerto > 1024/UDP)
hostname	DNS reverso del host
tag	Siempre será tftp
asn	ASN de la red donde se encuentra el host
geo	País donde se encuentra el host
region	Estado/Provincia/Región donde se encuentra el host
city	Ciudad donde se encuentra el host
naics	Código del Sistema de Clasificación Industrial de América del Norte
sic	Código del Sistema de Clasificación Industrial Estándar
opcode	Será “3” (significa que el archivo solicitado existe, en este caso a.pdf) o “5” (significa que el servidor TFTP retornó un código de error)
errorcode	Es el código de error que regresa con el opcode RFC1350/RFC2347
error	Versión del código de error. En el caso de una respuesta de código 3, es "No Error"
errormessage	El mensaje de error real que el servidor TFTP devolvió además del errorcode. En el caso de una respuesta opcode 3, es "File Exists"
size	Tamaño en bytes del payload de respuesta. Sólo es relevante en respuestas del opcode 3. Si el archivo está la respuesta será > 4 bytes

4. ACCIONES RECOMENDADAS

Para evitar este tipo de vulnerabilidad se recomienda que si no se necesita este servicio debe ser filtrado y si es indispensable su utilización se debe configurarlo adecuadamente teniendo en cuenta medidas de seguridad a nivel de aplicación.

5. REFERENCIAS

- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-TFTP
- https://tools.ietf.org/html/rfc1350
- http://protocoloftptftp.blogspot.com/
- http://www.csee.umbc.edu/~woodcock/cmsc482/proj1/tftp.html
- http://www.tavve.com/?literature=secure-tftp-proxy
- https://www.fi.upm.es/docs/servicios/seguridad_informatica/371_recomendaciones.pdf
- http://www.seguridad.unam.mx/noticia/?noti=2787
- https://www.us-cert.gov/ncas/alerts/TA14-017A