Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Passaggio 1: Installare VNC Server

Se non hai già installato un server VNC, installane uno. Ecco come fare su distribuzioni Linux comuni:

Debian/Ubuntu:

sudo apt update
sudo apt install tightvncserver

Red Hat/CentOS:

sudo yum install tigervnc-server

Passaggio 2: Configurare VNC Server

Configura il server VNC per creare un ambiente desktop per il client VNC.

1. Avvia il server VNC per configurare la password:

vncserver

2. Ti verrà richiesto di inserire una password. Assicurati che sia forte e composta da almeno 8 caratteri, includendo lettere maiuscole, minuscole, numeri e simboli:

Password:

Verify:

3. Ti verrà chiesto se desideri creare una password "view-only". Rispondi n per rifiutare.

Passaggio 3: Impostare una Password VNC Forte

Se vuoi modificare la password VNC in un secondo momento, puoi usare il comando:

vncpasswd

Assicurati di inserire una password forte seguendo le stesse linee guida descritte sopra.

Passaggio 4: Configurare il File di Avvio di VNC

Configura il file di avvio del VNC per utilizzare il desktop environment desiderato. Modifica o crea il file `~/.vnc/xstartup` e aggiungi il seguente contenuto (ad esempio, per utilizzare `xfce`):

#!/bin/sh

xrdb $HOME/.Xresources

startxfce4 &

Rendi il file eseguibile:

chmod +x ~/.vnc/xstartup

Passaggio 5: Configurare il Firewall

Assicurati che il firewall permetta il traffico VNC (porta 5901 per il primo display, 5902 per il secondo, ecc.). Apri le porte necessarie:

- **Debian/Ubuntu (con UFW):**

sudo ufw allow 5901/tcp

Red Hat/CentOS (con firewalld):

sudo firewall-cmd --permanent --add-port=5901/tcp

sudo firewall-cmd –reload

Passaggio 6: Avviare il Server VNC

Avvia o riavvia il server VNC con il comando:

vncserver

Passaggio 7: Configurazione Avanzata (Opzionale)

Per una sicurezza aggiuntiva, considera di utilizzare `ssh` per il tunneling del VNC. Questo aggiunge un ulteriore livello di cifratura alla connessione VNC.

1. Installa `openssh-server` se non è già installato:
    - **Debian/Ubuntu:**

sudo apt install openssh-server

Red Hat/CentOS:

sudo yum install openssh-server

Connetti al server VNC attraverso SSH tunneling dal client:

ssh -L 5901:localhost:5901 -N -f -l <username> <server_ip>

1. Connetti il client VNC a `localhost:5901` invece che all'IP del server.

Riepilogo

Seguendo questi passaggi, avrai protetto il servizio VNC con una password forte e configurato il firewall per consentire solo il traffico necessario. Considera l'utilizzo di SSH tunneling per una maggiore sicurezza.