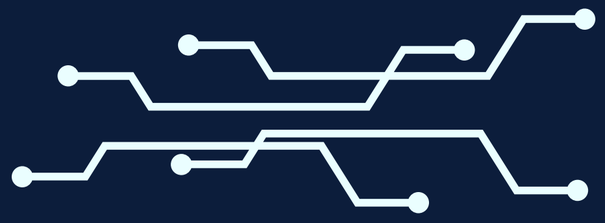
Exploit JAVA_RMI

An Introduction to M4 Project made by Mr.Federico Presti



About Java_RMI

The Java RMI to say fully, is a Server Insecure Default Configuration in the Java Code Execution

This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. Note that it does not work against Java Management Extension (JMX) ports since those do not support remote class loading, unless another RMI endpoint is active in the same Java process. RMI method calls do not support or require any sort of authentication

sources:
-http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.http
-http://www.securitytracker.com/id?1026215
-CVE-2011-3556.

Security Concerns:
Java RMI has been a target for vulnerabilities, especially when misconfigured or exposed to untrusted networks. Common risks include:

- RCE (Remote Code Execution): Attackers can exploit deserialization flaws to execute arbitrary code on the server.
- Insecure Configuration: Exposing the RMI registry or remote objects without proper access controls.

When used securely Java RMI is a powerful tool for building distributed systems in Java.

Security Concerns case:

The Nessus Vulnerability scan Plugin Overview

22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 C9 F1 82 65 00 00 01 93    Q....w.....e....
0x10:  45 F3 D2 AE 80 00 75 72 00 13 5B 4C 6A 61 76 61    E.....ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

Security Concerns case Alert:

The Nessus V.A tell no risk!

The previous page displays the RMI registry detection.

After having performed a thorough vulnerability scan on the host target of the M4 project, Metasploitable 2, i have no detected the Java_rmi vulnerability although it is reported in the NIST database with Base Score: 7.5 HIGH

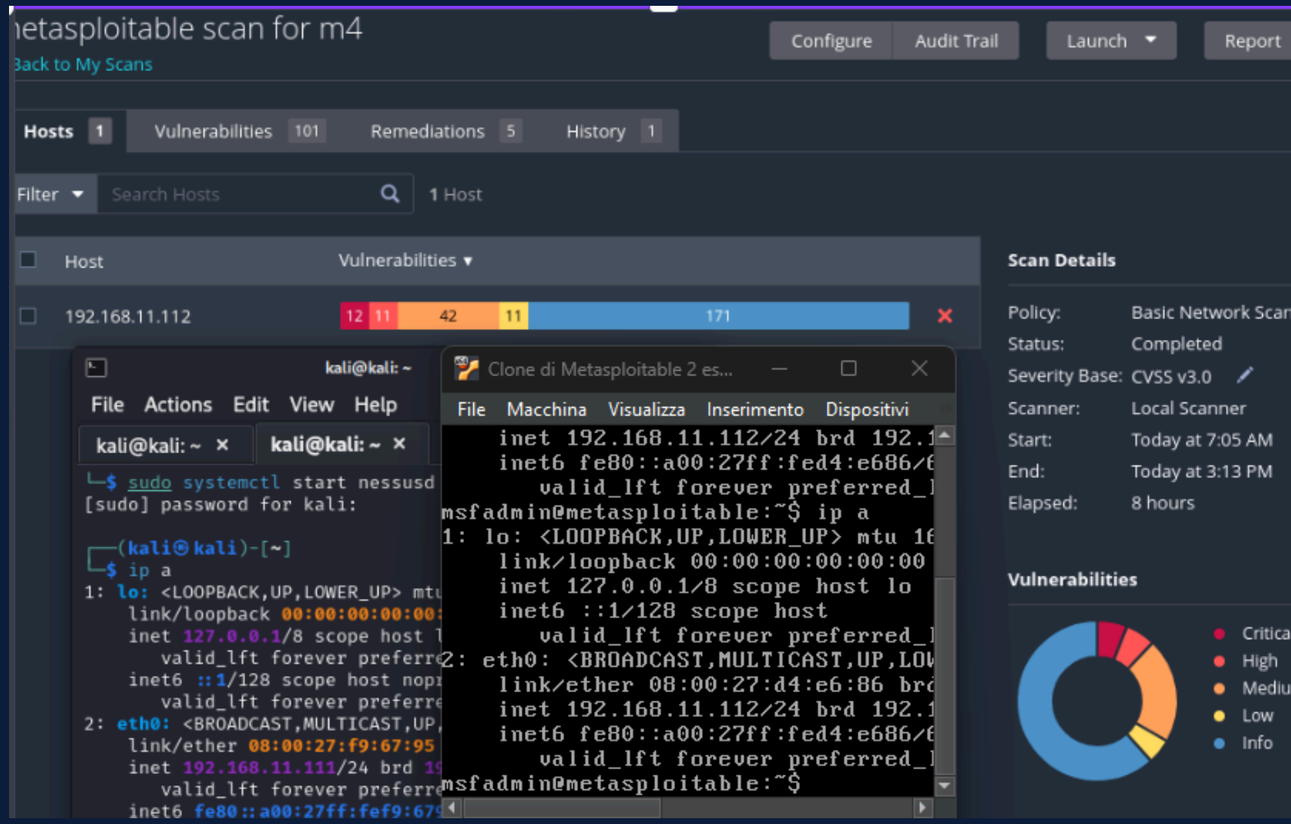
(https://nvd.nist.gov/vuln/detail/CVE-2011-3556)

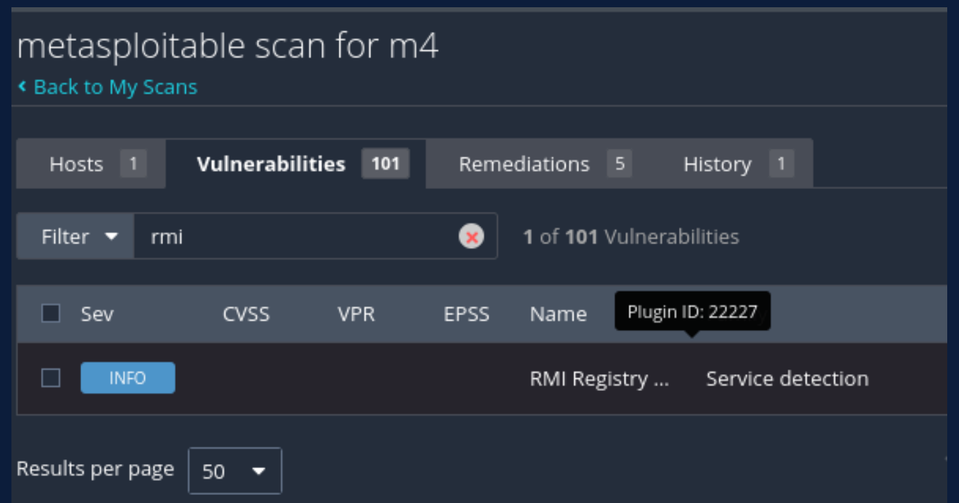
Nessus shows instead the Java R.M.I. registry, acronym for “Remote Method Invocation” with none risk factor.

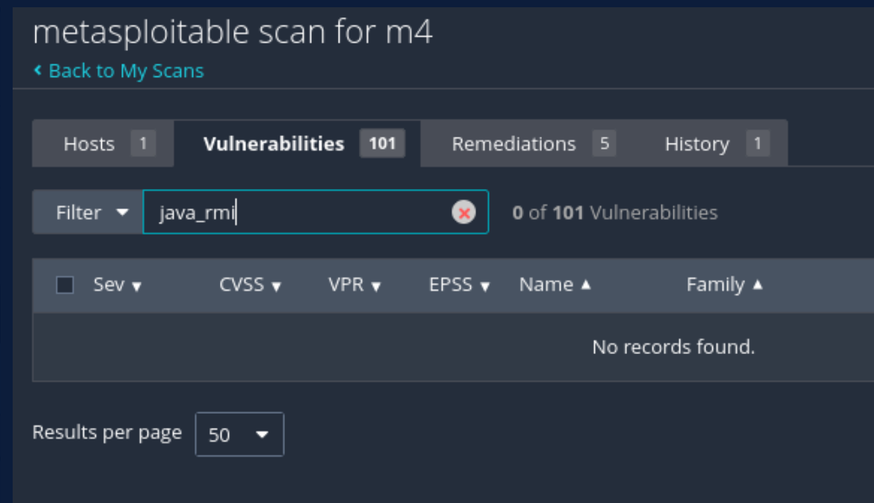
The RMI Registry and RMI Activation services are updated.. no risk!

Nessus proof of scan:

Nessus search for those vulnerabilities plugins:







.....but what if this would not be absolutely certain?

End of Introduction