Java RMI Server Insecure Default Configuration Java Code Execution

Disclosed10/15/2011
Created05/30/2018

Description

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 th RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used aga both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. Note that it do not work against Java Management Extension (JMX) ports since those do not support remote cla loading, unless another RMI endpoint is active in the same Java process. RMI method calls do n support or require any sort of authentication.

Author(s)

- mihi

Platform

Java,Linux,OSX,Solaris,Windows

Development

- Source Code
- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/misc/java_rmi_server
msf exploit(java_rmi_server) > show targets
    ...targets...
msf exploit(java_rmi_server) > set TARGET < target-id >
msf exploit(java_rmi_server) > show options
    ...show and set options...
msf exploit(java_rmi_server) > exploit
```