ProFTPD: Local privilege escalation

ProFTPD: Local privilege escalation LR

Flaw in the ProFTPD mod_ctrls module in versions

The load average on my insignificant personal firewall/server machine on my home ADSL line went through the roof a few days ago and a quick close-up inspection of it revealed that dozens of IPs from China and Taiwan were connecting to the FTP service. And the attempt kept on coming, and they still do.

Which is why I came up with these four lines,

```
ps uax|grep prof|grep -v grep|while read f;do
 i=`echo $f| cut -f 5 -d ":" |cut -f 1 -d "("`
 echo '$IPTABLES -A INPUT -i eth0 -s '$i' -j DROP'
done
```

...which prints out a nice list of currently connected users in a format which fits nicely in a firewall configuraion.

However, the obvious question is why? Why would they do this? Why attack some FTP? The answer much likely has somthing to do with this: It was ProFTPD version 1.2.10.

This version, and all versions previous to 1.3.0a, allows remote code execution in ProFTPD, possibly when only read access is given (as in anonymous logins allows) and definitively when write access is granted. (CVE-2006-5815)

The latest flaw, from February 13, 2007, is this:

0.1. mod_ctrls module flaw in ProFTPD versions <1.3.1_rc1

The flaw allows local users who have access to the mod_ctrls module, used by FTP server admins to configure the daemon at runtime, to obtain root privileges. (CVE-2006-6563)

The solution is to disable mod_ctrls or ensure only trusted users can access this feature or better, to upgarde to a 1.3.1rc1 (Released 12-Dec-2006) or a later version.

If you are using a ProFTPD version prior to 1.3.0a then you should definitively upgrade. Having your FTP targeted by a huge botnet in China is very bad indeed.

> Linux Reviews > News and headlines > 2007 News archive > March > ProFTPD: Local privilege escalation