

## Fw: init scripts and su

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-07/0037.html>

---

**From:** Nicolas Rachinsky (*list\_at\_rachinsky.de*)

**Date:** 07/26/04

Date: Mon, 26 Jul 2004 09:23:13 +0200

To: freebsd-security@freebsd.org

Hallo,

I think the same problem exists in our rc.d scripts.

Nicolas

***attached mail follows:***

---

Date: Mon, 26 Jul 2004 14:53:56 +1000

To: debian-devel@lists.debian.org

The start scripts for some daemons do "su - user" or use "start-stop-daemon -c" to launch the daemon, postgresql is one example.

During the time between the daemon launch and it closing it's file handles and calling setsid(2) (which some daemons don't do because they are buggy) any other code running in the same UID could take over the process via ptrace, fork off a child process that inherits the administrator tty, and then stuff characters into the keyboard buffer with ioctl(fd,TIOCSTI,&c) (\*).

To address these issues for Fedora I have written a program named init\_su.

init\_su closes all file handles other than 1 and 2 (stdout and stderr). File handles 1 and 2 are fstat()'d, if they are regular files or pipes then they are left open (no attack is possible through a file or pipe), otherwise they are closed and /dev/null is opened instead. /dev/null is opened for file handle 0 regardless of what it might have pointed to previously. Then setsid() is called to create a new session for the process (make it a group leader), this invalidates /dev/tty. Then the uid is changed and the daemon is started.

I have attached the source code to init\_su, please check it out and tell me

## FreeBSD-Security: Fw: init scripts and su

what you think. After the discussion concludes I will write a patch for start-stop-daemon to give similar functionality.

(\*) On system boot and shutdown there is no problem. It's when the administrator uses /etc/init.d/postgresql to start or stop the database that there is potential for attack.

<http://www.redhat.com/archives/fedora-devel-list/2004-July/msg01314.html>

I have also started a similar discussion on the Fedora development list about this issue, see the above URL.

--

<http://www.coker.com.au/selinux/> My NSA Security Enhanced Linux packages  
<http://www.coker.com.au/bonnie++/> Bonnie++ hard drive benchmark  
<http://www.coker.com.au/postal/> Postal SMTP/POP benchmark  
<http://www.coker.com.au/~russell/> My home page

--

To UNSUBSCRIBE, email to [debian-security-REQUEST@lists.debian.org](mailto:debian-security-REQUEST@lists.debian.org)  
with a subject of "unsubscribe". Trouble? Contact [listmaster@lists.debian.org](mailto:listmaster@lists.debian.org)

---

[freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org) mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "[freebsd-security-unsubscribe@freebsd.org](mailto:freebsd-security-unsubscribe@freebsd.org)"