

Re: [ronvdaal@zarathustra.linux666.com: Possible security issue with FreeBSD 5.4 jailing and BPF]

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-07/0031.html>

From: Ricardo A Reis (ricardo_bsd_at_yahoo.com.br)

Date: 07/14/05

Date: Thu, 14 Jul 2005 14:03:52 -0300

To: Avleen Vig <lists-freebsd@silverwraith.com>

I starting jail + devfs rules, in 5.4-STABLE using rc.conf. See the real entrie..

```
-----
jail_vhosts_rootdir="/usr/jail/vhosts"
jail_vhosts_hostname="vhosts.epm.br"
jail_vhosts_ip="127.0.0.3"
jail_vhosts_exec_start="/bin/sh /etc/rc"
jail_vhosts_exec_stop="/bin/sh /etc/rc.shutdown"
jail_vhosts_devfs_enable="YES"
jail_vhosts_fdescfs_enable="NO"
jail_vhosts_procfs_enable="YES"
jail_vhosts_mount_enable="NO"
jail_vhosts_devfs_ruleset="devfsrules_jail" -----"this use default
default devfs rule for best security in jail enviroment"
jail_vhosts_fstab=""
-----
```

In Jail i test your possible issue !!!

```
vhosts# ifconfig
r10: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=8<VLAN_MTU>
    ether 00:08:54:1a:68:b1
    media: Ethernet autoselect (100baseTX <full-duplex>)
    status: active
plip0: flags=108810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet 127.0.0.3 netmask 0xffffffff
pflog0: flags=141<UP,RUNNING,PROMISC> mtu 33208
vhosts# tcpdump -nni r10
tcpdump: (no devices found) /dev/bpf0: No such file or directory
vhosts# tcpdump -nni lo0
tcpdump: (no devices found) /dev/bpf0: No such file or directory
```

Atenciosamente

Re: [ronvdaal@zarathustra.linux666.com: Possible security issue with FreeBSD 5.4 jailing and BPF]

Ricardo A. Reis
UNIFESP – SENAI
Unix and System Admin

>This message was sent to bugtraq today:

>

>

>While playing around with FreeBSD 5.4 and jailing I discovered that it was
>possible to put an ethernet interface into promiscious mode from within the
>jailed environment, allowing a packetsniffer to gather data not meant for
>the jailed box. This also affects FreeBSD 5.3 (tested) but not FreeBSD 4.x
>This can be reproduced on boxes where BPF support is enabled in the kernel
>and a BPF device is available in the jail (badly configured devfs/no rules)

>

>The problem lies within the FreeBSD 5.x BPF kernel code:

>

>"The Berkeley Packet Filter provides a raw interface to data link layers
>in a protocol independent fashion. The function bpfopen() opens an
>Ethernet device. There is a conditional which disallows any jailed
>>processes from accessing this function."

>

>This conditional was present in the 4.x series kernels but is missing
>in 5.x and thus allowing free access to bpfopen() from within a jailed
>environment. I think this is related to the changed jailing code between
>these kernels. I don't believe this has been left out on purpose in favor
>of devfs rulesets (...) If not, I'd like to have some comments on this.

>

>

>Example:

>

>jail# uname -a

>FreeBSD jail 5.4-RELEASE FreeBSD 5.4-RELEASE #0: Sun May 8 10:21:06 UTC
>2005 root@harlow.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386

>

>The ethernet interface of the host (parent) is not in promiscious mode.

>The interface of the jailed environment isn't in promiscious mode either:

>

>jail# ifconfig | grep fxp0

>fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500

>

>

>Now starting tcpdump in the jail:

>

>jail# tcpdump -i fxp0

>tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

>listening on fxp0, link-type EN10MB (Ethernet), capture size 96 bytes

>

>

>Checking the interface again within the jail:

>

>jail# ifconfig | grep fxp0

FreeBSD-Security: Re: [ronvdaal@zarathustra.linux666.com: Possible security issue with FreeBSD 5.4 jailing and BPF]

>fxp0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500

>

>The interface is running in promiscuous mode.

>

>

>The host environment shows that the tcpdump process runs in a jail:

>

>root@nietzsche# ps aux|grep tcpdump

>root 50551 0.0 0.9 3784 2248 p4 S+J 8:37PM 0:00.04 tcpdump

>- -i fxp0

>

>The P_JAILED flag is set.

>

>

>Conclusion:

>

>Usage of devfs rulesets is highly recommended as stated in the manpages.

>Though a misconfiguration at this point would expose a big security issue.

>The question is: should bpfopen() in bpf.c check for a jailed proc or not?

>

>

>Grt,

>

>Ron van Daal

>

>_____
>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"

>

>

>

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"

Re: [ronvdaal@zarathustra.linux666.com: Possible security issue with FreeBSD 5.4 jailing and BPF]