

Re: Closing information leaks in jails?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-08/0023.html>

From: Nate Nielsen (*nielsen-list_at_memberwebs.com*)

Date: 08/19/05

To: Attila Nagy <bra@fsn.hu>

Date: Thu, 18 Aug 2005 22:44:42 +0000 (GMT)

Attila Nagy wrote:

> *Hello,*

>

> *I'm wondering about closing some information leaks in FreeBSD jails from the "outside world".*

>

> *Not that critical (depends on the application), but a simple user, with restricted devfs in the jail (devfsrules_jail for example from /etc/defaults/devfs.rules) can figure out the following:*

>

> *– network interfaces related data, via ifconfig, which contains everything, but the primary IP address of the interfaces. It seems that alias IPs can be viewed:*

> *bge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500*

> *options=1a<TXCSUM,VLAN_MTU,VLAN_HWTAGGING>*

> *ether 00:12:79:3d:83:c2*

> *media: Ethernet autoselect (100baseTX <full-duplex>)*

> *status: active*

> *lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384*

> *inet 127.0.0.2 netmask 0xff000000*

For me this only shows the alias assigned to the jail.

> *– full dmesg output after boot and the kernel buffer when it overflows*

> *(can contain sensitive information)*

Yes, this is important. Use:

`sysctl -w security.bsd.unprivileged_read_msgbuf=0`

> *– information about geom providers (at least geom mirror list works)*

> *– the list of the loaded kernel modules via kldstat*

> *– some interesting information about the network related stuff via netstat*

netstat works, but it limits itself to the jail pretty well. In particular 'netstat -r' and friends don't work. The normal 'netstat -a' only shows connections to the current jail. It does show the output from 'netstat -m' and those sort of things, but those say nothing over the

FreeBSD-Security: Re: Closing information leaks in jails?

network load of the current machine.

> – *information about configured swap space via swapinfo*

Not sure I see how this could be used against you.

> – *NFS related statistics via nfsstat*

Again only statistics. Not sure how this is a problem.

> – *a lot of interesting stuff via sysctl*

Yes, there's a lot there, but a lot **is** filtered out in a jail.

> *Are there any ways to close (some of) these?*

My suggestion would be to file bugs one by one for each piece of information that causes you concern along with the reasoning of why that information is dangerous or sensitive.

The FreeBSD developers have been attentive to these things, and have added functionality in almost each release to minimize information available in a jail. So pointing specific issues out will probably get good results.

Cheers,
Nate

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"