

Re: Closing information leaks in jails?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-08/0021.html>

From: Attila Nagy (*bra_at_fsn.hu*)

Date: 08/18/05

Date: Thu, 18 Aug 2005 17:46:58 +0200
To: Benjamin Lutz <benlutz@datacomm.ch>

Benjamin Lutz wrote:

>>– *full dmesg output after boot and the kernel buffer when it overflows*
>>*(can contain sensitive information)*

> *If it's sensitive in so far as it endangers the privacy of local*
> *non-jailed users, I think that's a bug that'd need fixing.*

There are many points from this issue can be observed. Let's take a shell server, or a CGI server. Take the latter for an example.

> *I'm not sure why hiding the mentioned information is bad. It only*
Not bad at all. The bad thing is that they are available and the administrator can't (AFAIK, without any hacking) hide them. :)

> *contains machine-specific data, and at best the private information a*
> *jailed user will be able to figure out is the machine's usage patterns*
> *(yes, crypto folks don't like that, but c'mon...). Hiding that data*
> *isn't real security.*

Hmm. Why ifconfig doesn't tell me the main IP address of an interface?
BTW, this is not usage pattern, and ARP data (MAC addresses, you can do interesting stuff with them, for example guess what kind of operating system and hardware run the given IP, etc) is not either.

And not showing the MAC and IP addresses for all of your users can be real security.

> *Besides, the user can only gain the data if he can execute the binaries*
> *that provide it. Why not remove, say, the geom programs (and at the same*
> *time make it impossible to execute new programs? Eg only make the*
> *home/tmp dirs writeable, but put those on a noexec partition). That*
> *should make it hard enough to access geom data.*

As I said there are many different cases. In the case of a CGI server, you must make those executables executable. And the worst part is that your users can modify them without too much control.

In another example, when you would like to provide "virtual machines", where the user can manage his jail, this "solution" is also not good.

I think it is pointless to ask why would hiding the ARP table, or the

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

system's IP addresses is sane or not, when currently you can't do a netstat -an from inside a jail and also can't do many other things.

Oh, and you can do iostat! :)

--

Attila Nagy

e-mail: Attila.Nagy@fsn.hu

Adopt a directory on our free software

phone @work: +361 371 3536

server! <http://www.fsn.hu/?f=brick>

cell.: +3630 306 6758

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"