

Re: FreeBSD Security Advisory FreeBSD–SA–05:21.openssl

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-10/0041.html>

From: jere (*jere_at_htnet.hr*)

Date: 10/12/05

Date: Wed, 12 Oct 2005 12:09:53 +0200

To: Timothy Smith <timothy@open-networks.net>

Please read these articles/manuals:

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/small-lan.html

http://2004.eurobsdcon.org/uploads/media/EBSD04_27.pdf

http://www.taosecurity.com/keeping_freebsd_applications_up-to-date.html

http://www.taosecurity.com/keeping_freebsd_up-to-date.html

These are very helpful articles on this matter and it seems every large environment should have a big-bytecrunching-beast-server(s) to do the dirty job of building OS and making packages you'll use. Another thing is if you have same or similar hardware (today's blade servers come to mention here) the whole process is focused to building just few (or just one) OS/kernel versions you can instantly install on any production server say via NFS (as explained in above articles) over isolated LAN segment dedicated to this, if you want additional security and reliability. Let's say it **is** possible to automate OS security patching to some reasonable degree this way even in large environments but you don't have this feature "out-of-box" – you have to build it yourself. Beleive me, large environments like "out-of-box" solutions. :)

And there lies another problem. In large environments it is also difficult to manage packages security issues. The problem is updated port tree not just necessariliy fix the security issue – it often also bumps version of affected package – something not always needed in production and most often avoided. The first concern of production (enterprise or not) should be stability. For example, one can use build server to quickly build new packages but that package may be automatically bumped to newer version – with patched security issue and new features added. Currently FreeBSD admins don't have a clear choice to manage only ports security issues but I think it's primarily due to lack of port maintainers.

Does anyone have other thoughts about this?

j.

Timothy Smith wrote:

> *jere wrote:*

>

>> *unfortunately, this is the dark side of FreeBSD security patch
>> management :) and I think also the main reason FreeBSD isn't so
>> widely deployed into enterprise environments. It's ok for hacking or
>> managing few boxes but try to imagine how to manage security on
>> hundreds of them this way. :(*

>>

>> *on the other side (bright side :) you can try to use unofficial and
>> often somewhat slowly updating solutions such as bsdupdate
>> (www.bsupdates.com) or freebsd-update (from ports tree).*

>>

>> *currently, FreeBSD just don't have a mechanism to handle security
>> advisories in quick way.*

>>

>> *any suggestions/corrections ?*

>>

>> *j.*

>>

> *your totally right, even though i hate to admit it. stuff like having to
> make world is a nightmare when admining lots of machines. i can't afford
> to make world only to find something screwed up, stuff like that would
> cost me a lot of time i can't afford.
> the make world documents mentioning backing up your system. it fails to
> give any preffered methods or utilites for doing this. anyone got some
> input on that.*

>

> 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"