

Re: Redhat and OpenSSL Manner

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-12/msg00305.html>

- *From:* Aleksandar Milivojevic <alex@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 21 Dec 2006 09:02:21 -0600
-

Quoting Vahric MUHTARYAN <vahric@xxxxxxxxxxxx>:

Hello ,

We are scanning our web servers for vulnerability but I have a problem on one thing. I red that redhat never change version of openssl but it's updating . it just only add additional numbers behind of packet. like below but I don't know is this version equal to 0.9.7i or 0.9.8d . Anybody have knowledge about it ?

openssl-0.9.7a-43.14

It's equivalent to 0.9.7a as originally distributed by OpenSSL project, with security and bug fixes added to it by Red Hat. The package is always built from version of source it is claiming to be, with security and bug patches applied to it.

The rule of thumb is, the version is always what it says it is. With security and bug fixes backported from newer versions. In some cases, enhancements and new features might be backported from newer versions too if they are not introducing any compatibility problems (for example this is often done for kernel package in RHEL to support new hardware). Notice the keyword "backported" that I used. Red Hat does not use new version of the source code. They just reimplement fixes into the old version as a series of patches. If you look into the SRPM packages, you'll see that they contain original unchanged source code which is the same version as the package version, and also bunch of patches (security and bug fixes) that get applied to that source code prior to compilation.

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxxx?subject=unsubscribe>

<https://www.redhat.com/mailman/listinfo/redhat-list>