DISCLAIMER! This document is nothing more than the musings of the author as he attempts to perform the stated tasks. Conclusions and approaches may very well be incorrect, inefficient, or otherwise outside of professionally accepted best practices. Use this document at your own risk! In this document, screen outputs will be presented in **green**. Where keyboard input is required, the prompt will be in bolded red. **#** means you should be at the super user prompt, **$** means you should be at an unprivileged user prompt. Do not include these prompts in your input! The command to be typed will be shown in **blue**.

 # ls -al

means you type ls -al at the super user prompt.

Does the Oracle Critical Patch Update maintain Firefox for IAVA Compliance ?

Historically, the Mozilla Foundation Firefox web browser has had monthly security vulnerabilities associated with with it. To mitigate the risks, I would download and install the latest contributed package for Solaris 10 from the Mozilla FTP site. As of this writing, the latest contrib package is v31 while the latest version of Firefox is v36.

Relying on 3rd party contrib packages does not seem to be an option going forward. I asked if anyone on the Linkedin Solaris group had experience compiling new releases of Firefox from the source code. One respondent suggested that I let Oracle's patches take care of upgrades. I inherited the upgrade process from a very smart engineer, who left our organization. He was quite thorough in his efforts, so I used his method to upgrade Firefox without further thought.

To qualify his approach, I want to test it against using the Oracle CPU process for upgrading.

Testing

Objective: The intent of this test is to determine if the Critical

Patch Upgrade for Solaris 10 maintains the 'as delivered' package from Oracle's Solaris 10 installation media.

I uninstalled (pkgrm) the packages I had for Firefox and Mozilla (determined by *pkginfo | grep -i mozilla and pkginfo | grep -i firefox*) and installed the package contained in the Product directory of the Solaris 10 Upgrade 11 1/13 installation dvd (*SUNWfirefox*).

The version of that firefox browser is 10.0.7. The remainder of the system is the Solaris 10 Update 11 operating system with the Oct 2014 CPU patches applied. The test was performed on a SunBlade 2500 sparc workstation. The uname -a output is:

SunOS 10adm 5.10 Generic_150400-17 sun4u sparc SUNW,Sun-Blade-2500

Applying Patches

Not wanting the results to be based on the application of a specific patch of my choosing, I applied the entire 10_Recommended patch set from the OCT 2014 CPU (latest release as of this writing) instead of just installing the 145080-14 patch which identifies itself as a firefox patch. The next CPU release is due on the 20th of January. I will apply that patchset to further assist in my conclusions.

This system has already had the October 2014 CPU update applied so the assumption is, any patches applied in this test are related to upgrading Firefox.

Following patches were applied :

123893-77 125136-85 125137-85 145080-14

Firefox prior to patching:

 # firefox -v

Mozilla Firefox 10.0.7 ESR

after patching:

 # firefox -v

Mozilla Firefox 24.2.0 ESR

some caveats to the above results. I was not truthful when I said the only change to the system was to update firefox. I had attempted to compile firefox, so had installed the autoconf package and upgraded to python2.7.

Exploring the patches that were applied:

123893-77 - SunOS 5.8 5.9 5.10: Common Agent Container (cacao) runtime 2.4.3.0 upgrade patch 77 (dont' know why it applied this time)

125836-85 - JavaSE 6: update 85 patch (equivalent to JDK 6u85)

125837-85 - JavaSE 6: update 85 patch (equivalent to JDK 6u85), 64bit

145080-14 - SunOS 5.10: Firefox patch

I assumed 145080-14 would be installed. I do not know why the CAC and Java patches decided to apply this time, but they don't seem to have had influence on Firefox.

Conclusion

- **If the installed firefox is from the original Oracle Solaris 10 1/13 media package, the CPU process will upgrade to the latest patchset supported by the vendor. However, the effect of the CPU is not sufficient to meet DoD IAVA compliance.**

- **Often, the IAVA allows mitigation pending OEM packages. If this is allowed, un-installing 3rd party packages and installing the OEM package will facilitate mitigation.**

- **If not, and absent the availability of 3rd party packages, compilation of Firefox source code is the only solution for meeting IAVA compliance.**