Finding Security holes early with FLRTVC
By Jaqui Lynch

No matter what IT magazine you pick up today, one of the key topics covered will be security. Today it is critical to close any security holes as quickly as possible so that hackers are less able to take advantage of them. With FLRT (fix level recommendation tool) IBM started the process by allowing clients to check that they were installing compatible levels of code. They then added links to the AIX/VIOS Security and Hiper Tables. The latest iteration is the introduction of FLRTVC (FLRT Vulnerability Checker).

FLRTVC comes in two flavors – the first is a script that you can run on the system that uses data from a file (apar.csv) to compare installed filesets and interim fixes against known security problems. The second option is to use the web based online tool (FLRTVC Online). This option allows you to upload the output from two commands to the web page and it produces the output that you need to identify security holes that need to be closed.

FLRTVC Online
In order to use this option you will need to logon to the system you want to check and run the following two commands:
lslpp –Lcq >lslpp.txt
sudo lslpp –e >emgr.txt

You then move the two files to a system with a web browser, go to the FLRTVC Online webpage and upload the two files, select the APAR type (I choose All) and then click on “Run vulnerability checker”. APAR Type options are All, High impact pervasive (HIPER) and Security. The system then produces a report that identifies the vulnerabilities that it found and the actions to be taken.

FLRTVC Script
Of the two options this is the easiest one to automate. The script downloads the apar.csv file from the FLRT website using CURL or WGET. If you don’t have either of these then you need to download the file yourself prior to running the script. The apar.csv file (if you download it) needs to be in the same directory as the script. Once the file is downloaded you can run the script manually or you can set up cron to run it periodically. The script should be run after any system maintenance to double check for newly introduced issues.

The script runs the lslpp commands listed above and then compares them to the vulnerabilities listed in the apar.csv file. Output is in either compact or full (verbose) mode with the default being compact. Compact produces a csv delimited (by |) file that can be read into a spreadsheet. Verbose mode is suited for use when you want something that is to be emailed out in human readable format. When I run flrtvc I take all the defaults so that I get everything in compact mode which I can then download and view in a spreadsheet.

To run flrtvc you first need to download the .zip file and then unzip it. You may also need to download the apar.csv file if wget or curl do not work. Once that is done you can run it in compact mode and produce an output file as follows:
cd /directory where flrtvc is
ksh93 ./flrtvc.ksh >systemname-flrtvc-output.csv
Then ftp or scp as asci the systemname-flrtvc-output.csv file to your computer and open it with Excel as a .csv file – the delimiter is |. There are a number of flags that you can use but for the most part I use none of them as I want to get everything.

I tend to have the output go to an NSF mounted filesystem so that all of my security reports are in one place. That way you can concatenate them together or at least just download them all from one place. You can also write scripts that grep on certain things in the output and email those to yourself.

The compact output from the FLRTVC script is best viewed in a spreadsheet and is broken down into the following columns:
Fileset, Current version, EFix, Abstract, Unsafe versions, APARs, Bulletin URL, and Download URL.

Fileset shows the name of the fileset that is of issue i.e. bos.net.tcp.client
Current Version shows the currently installed level i.e. 7.1.3.45
Type will be either sec (for security) or hiper.
EFix – this confused me at first. It turns out that you only see a value here if the actual efix for the problem is installed – I thought it was the name of the efix to be installed at first. So, if you see something in this field then it means you have the efix on and should be able to see it using emgr –e or lslpp –e.
Abstract is a description of the problem i.e. Vulnerability in BIND
Unsafe Versions is a list of the fileset levels that are impacted i.e. 7.1.3.0-7.1.3.45
APARs provide that actual APAR number i.e. CVE-2015-5477 or IV75031
Bulletin URL provides the URL where you can go to read about the vulnerability to get more information i.e.
https://aix.software.ibm.com/aix/efixes/security/bind9_advisory8.asc
Download URL is the URL where you can go to download the actual efix for the problem i.e. https://aix.software.ibm.com/aix/efixes/security/bind9_fix8.tar although sometimes it will just say “see advisory”.

The next step is to go through each of the vulnerabilities found and to determine which ones to put on. Then you download the necessary fixes and install them. It is important that you carefully read the advisory to ensure you install the correct fix. As an example, there is a nettcp set of fixes
(see https://aix.software.ibm.com/aix/efixes/security/nettcp_advisory.asc)
This is a group of fixes for ftpd, sendmail and popd/imapd. Altogether there are three fixes to go on in this one advisory.

As you read the advisory you should first check the “AFFECTED PRODUCTS AND VERSIONS” section – here it shows you the lower and upper levels of the fileset that are impacted. If your fileset is at any of these levels then you need to look at the “REMEDIATION” section to determine the exact APAR or APARs to install. When you download the fix it will potentially include the APARs for different levels of AIX 6.1 and 7.1. As an example, the ftpd fix above has 4 different efixes depending on whether you are at 6.1.8.7, 6.1.9.6, 7.1.2.7 or 7.1.3.6. Just below the list of APARs in the REMEDIATION section you will also find links to subscribe to the APARs – since these are efixes that have to be removed before doing any future maintenance then you should subscribe to the APARs so that you are notified when the full fix becomes available.

Once the fixes are downloaded and the file is untarred, and you have identified the correct APARs you can then install the efix. There are instructions in the advisory in how to check the signature, etc to ensure you have downloaded the file correctly. To install the APAR you should first run the install in preview mode: For the bind9 patch I used the 7.1 efix as follows:
emgr -p -e IV75693s5a.150803.epkg.Z
If it comes back successful it will also tell you whether or not it needs a reboot after the efix is installed. To actually install the patch you remove the –p as follows:
emgr -e IV75693s5a.150803.epkg.Z
When installing certain products (such as samba or sendmail or ssh) you may have to stop and start the applications to ensure the updates are activated.

When you have finished installing the updates it is then time to run emgr –l (or lslpp –e) to get the list of patches installed. You will get a list that looks something like:

emgr -l

```
ID  STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ==========
====================================
1   S   IV71446m9a 04/16/15 12:52:00      Ifix for Openssl CVE                 Openssl
2   S   IV77299s5b 10/19/15 15:49:12      Fix for CVE-2015-4948                Netstat
3   S   IV75646m5a 10/25/15 09:43:38      IV75646 for AIX 7.1 TL03 SP05        sendmail
4   S   IV73975s5a 10/25/15 09:46:55      IV73975 for AIX 7.1 TL03 SP05        nettcp
5   S   IV73316s5a 10/25/15 09:48:09      Ifix for IV73316 at AIX 7.1 TL03 SP05.       nettcp
6   S   IV74261s5a 10/25/15 09:49:44      ifix for CVE-2015-1799               ntp
```

One other point to note is that some of these patches, especially the openssl ones, require a certain level of the application to be installed for the patch to go on. As an example, for openssl two of the patches affect openssl 1.0.1.500-1.0.1.513 and one of them is for openssl 1.0.1.500-1.0.1.514. In order to install the patch you have to bring openssl up to the highest level (either 513 or 514 depending on the patch). These are not always easy to find.

Summary

FLRTVC is a great new tool to have in your kit to help ensure that security remediation is done as quickly as possible. It provides in one file a description of the problem, the filesets impacted, links to the fixes and bulletins and whether or not the efix is actually installed. There are a couple of things I would like to see added such as a link to where to download that fileset if you have to have the highest level one and a link to follow the apar. But this tool is incredibly useful as is and should be in all of our toolkits as we try to keep our systems secure.

Finally, the team supporting FLRTVC is continuing development and would greatly appreciate any feedback. Feedback goes directly to the developers at the feedback link below.

References

FLRTVC Feedback Link
http://www14.software.ibm.com/webapp/set2/feedback

FLRT Home Page
https://www14.software.ibm.com/support/customercare/flrt/
or https://ibm.biz/IBM-FLRT

FLRTVC Home Page
https://www14.software.ibm.com/webapp/set2/sas/f/flrt/flrtvc.html
or https://ibm.biz/IBMFLRTVC

Flrt Wiki
https://ibm.biz/FLRTWIKI

Apar.csv file
https://www14.software.ibm.com/webapp/set2/flrt/doc?page=aparCSV

FLRTVC Online Tool
https://www14.software.ibm.com/webapp/set2/flrt/vc

AIX VIOS Security Tables
https://www14.software.ibm.com/webapp/set2/flrt/doc?page=security

AIX VIOS HIPER Tables
https://www14.software.ibm.com/webapp/set2/flrt/doc?page=hiper

FLRTVC 0.4 Download
https://www14.software.ibm.com/webapp/set2/sas/f/flrt3/FLRTVC-0.4.zip

Flags for flrtvc (taken from FLRTVC Home Page)
-d = Change delimiter for compact reporting
-f = File selection for *.csv file

-q = Quiet mode, hide compact reporting header
-s = Skip download, use default apar.csv file
-v = Verbose, full report (for piping to email)
-g = Grep for filesets with phrase, useful for verbose mode
-t = Type of APAR [hiper | sec]
-l = Enter a custom LSLPP output file, must match lslpp -Lqc
-e = Enter a custom EMGR output file, must match lslpp -e
-x = Skip EFix processing