Technical Information Bulletin

TIBID# DSI140916
Date: 09/16/2014
Importance: High

Title: VMware Library controller requires a patch to address Heartbleed Vulnerability

Description of Problem: ESXi version 5.5 is vulnerable to CVE-2014-0160

Solution: Apply instructions below to install VMware patch ESXi550-201404001 to vulnerable systems. This will update OpenSSL to version 1.0.1g which is not vulnerable to the Heartbleed vulnerability.

Any questions about this TIB should be directed to DSI support at the following email address.

SUPPORT@DYNAMICSOLUTIONS.COM

Thank you;
DSI
Customer Support
(800) 641-5215

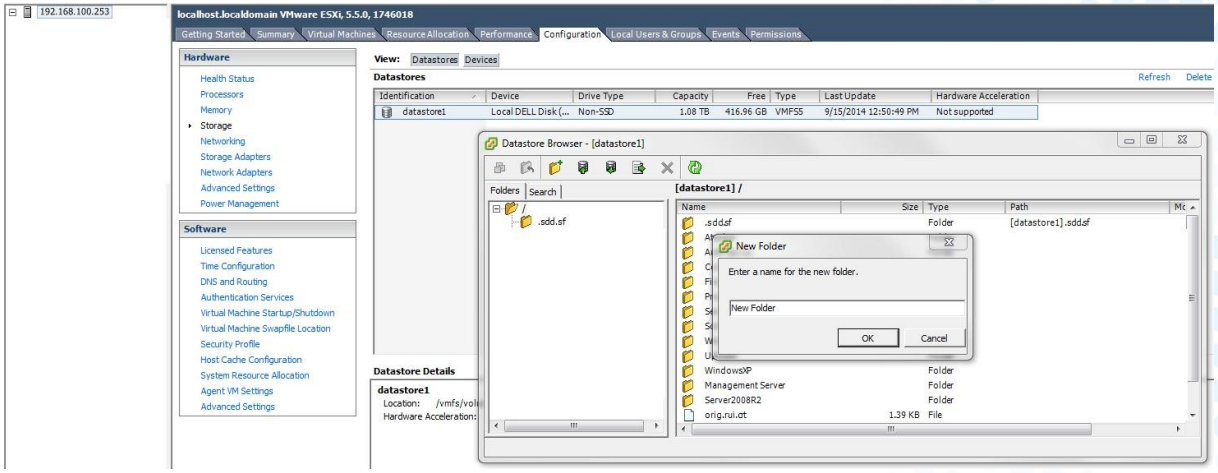
ESXi Heartbleed update on DSI1000 IPV Controller

1. Download the patch located on the DSI support site.

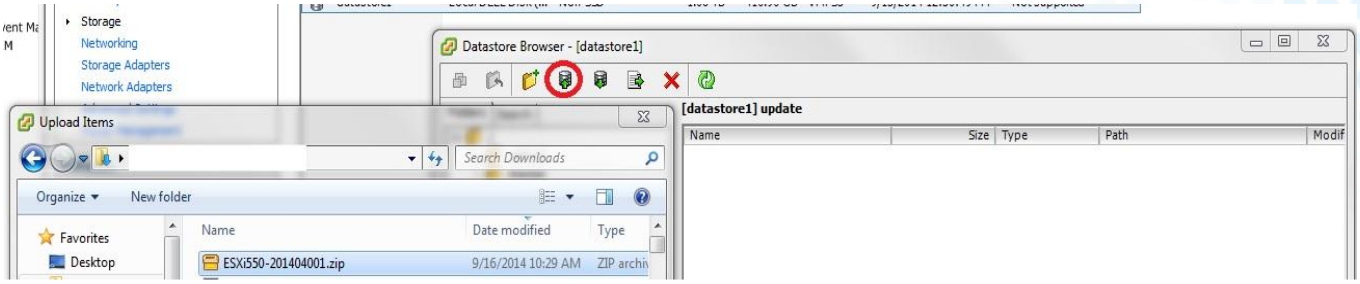
   ftp://ftp.dynamicsolutions.com/DSIStorage/Controllers/IPV_Patches/

2. In this case the patch is: **ESXi550-201404001.zip**

3. Move the .zip file to the datastore of the ESXi host
   a. Through vSphere client
      i. Configuration Tab > Storage > Datastore1
      ii. Right click datastore1 & Browse Datastore
      iii. Click on the root directory & Create new Folder called “update

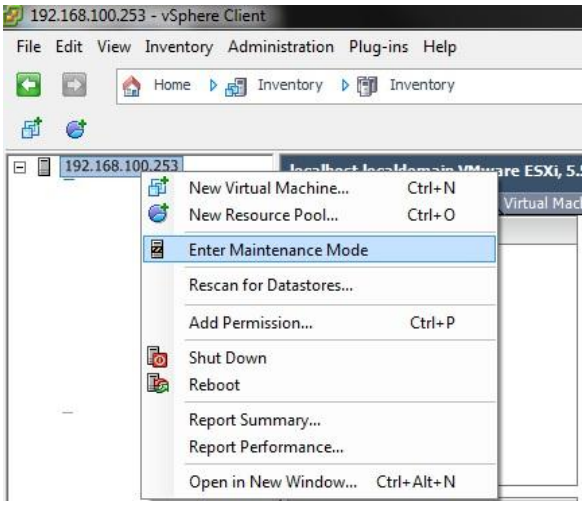


   iv. Open the update directory and Click the Upload Icon, choose “file”
   v. Move the .zip file downloaded in step 2 into the update folder.

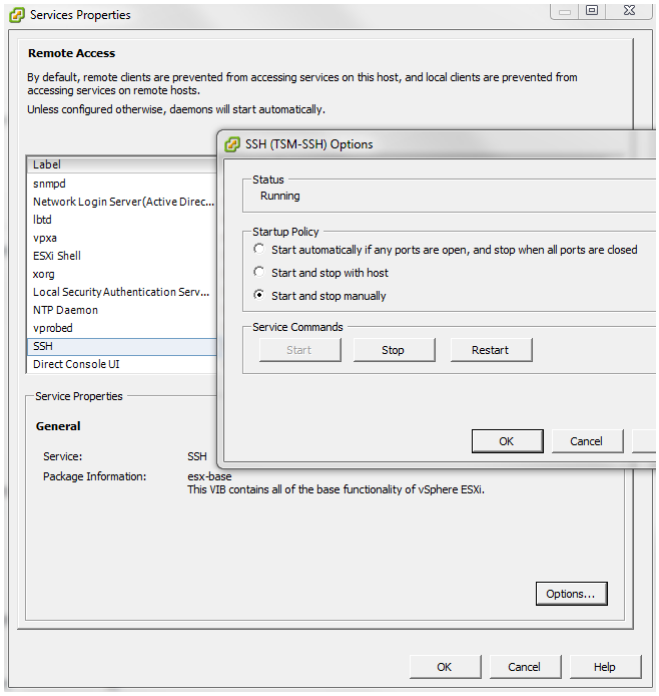


4. Power off All virtual machines

5. Place the ESXi server in maintenance mode
    a. Right click on the ESXi server name & select maintenance



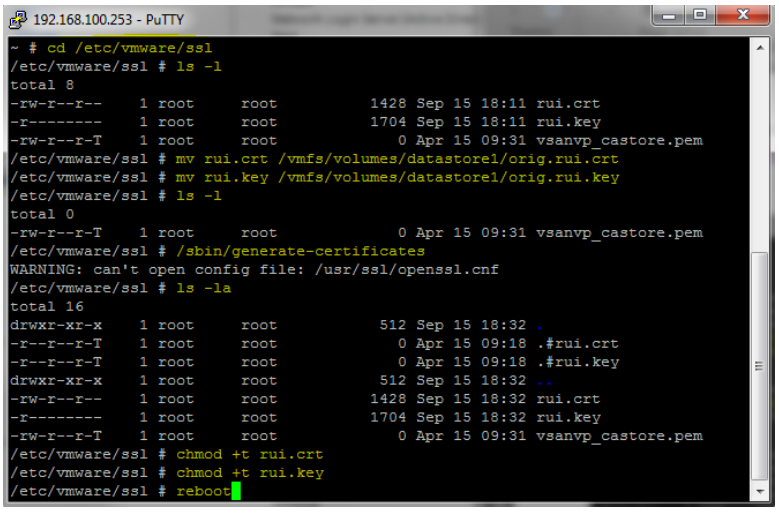
6. Through the vSphere console enable SSH
    a. Configuration tab > Security Profile > Services Properties
    b. Select SSH & click options
    c. Start the SSH service



7. Connect as “root” using putty or similar tool to the ESXi host
    a. Run these commands
        i. esxcli software vib update --depot= /vmfs/volumes/datastore1/update/ESXi550-201404001.zip
        ii. reboot
8. Log back in with putty as root and verify SSL is no longer running a vulnerable version
    a. Type these commands
        i. openssl version
            - You should now be running a version later than 1.0.1f

9. Finally to re-create certificates run the following commands
    a. `cd /etc/vmware/ssl`
    b. `mv rui.crt /vmfs/volumes/datastore1/orig.rui.crt`
    c. `mv rui.key /vmfs/volumes/datastore1/orig.rui.key`
    d. `ls -l`
        i. Confirm the certificates have been moved
    e. */sbin/grenerate-certificates*
        i. *Ignore the warning dialog after this command*
    f. *ls –la*
        i. Verify new certs created with updated timestamps

    g. `chmod +t rui.crt`
    h. `chmod +t rui.key`
    i. `reboot`



The warning is ok after running the generate-certificates command

10. Log back into vSphere and accept security warning

11. Stop SSH access.
    a. Configuration tab > Security Profile > Service properties
    b. Select SSH & click options
    c. Stop SSH
    d. Click “OK”

12. Take server out of maintenance mode
    a. Right click server name
    b. Click exit maintenance mode

13. Power on all virtual machines
    a. Right-click
    b. Power on virtual machine

Contact Info:

All questions or concerns regarding this document, should be directed to support@dynamicsolutions.com or (800) 641-5215.