Shellshock Security Patch for X86

Guide for Using the FFPS Update Manager

October 2014

Version 1.0

This page is intentionally blank

Table of Contents

This page is intentionally blank.

1.0 Overview - Shellshock/Bash shell Vulnerability

Summary:

On Sept 25th, media sources announced security vulnerabilities in the Bash shell software (aka Shellshock). Understandably, Xerox customers are concerned about these vulnerabilities.

Unix and Unix-derived systems like Linux and Mac OS X are vulnerable to these attacks since they use Bash as the default command shell. The FreeFlow Print Server (FFPS) includes the Solaris Operating System, which is potentially affected since it includes the Bash shell.

Risk Assessment:

On a product that exposes the Bash shell to the network, the vulnerabilities could allow attackers to remotely execute commands on a target system. .

FFPS Engineering has evaluated the bash vulnerabilities and believes the risk of exposure for the DocuSP/FreeFlow Print Server software is very low. The rationale for this is:

1. Bash is not used as a default shell for any remote connection and is not used for SSH
2. The FFPS Web Server does not permit remote execution of CGI/shell commands
3. FFPS Workflow and Printing protocols do not use Bash
4. When FFPS is running with standard security settings, remote connections to Solaris applications are greatly restricted.

Patch Delivery Plan:

The Bash patch is available for FFPS (see sections below). The patch is not mandatory but it is recommended to be installed since in the future, this patch may be needed if additional vulnerabilities are found in the Bash shell. The patch will be included in future releases of the FFPS Quarterly Security Patch cluster deliveries. Customers with Digital Front End products (DFEs) running FFPS v7, v8, and v9 have the ability to download and install the Bash patch using the FFPS Software Update Manager. Customers with DocuSP v5 and FFPS v6 should contact their local Xerox Service representative to request the patch be installed at the next scheduled Service visit.

The Security vulnerabilities that are remediated with this FFPS Security patch delivery are as follows:

1. CVE-2014-6271
2. CVE-2014-7169
3. CVE-2014-7186
4. CVE-2014-7187
5. CVE-2014-6277
6. CVE-2014-6278

2.0 Introduction to Network Delivery of Software Updates and Patches

FreeFlow Print Server Software Update Manager is included in FFPS versions 7, 8, and 9. It is also included in these Nuvera Products: Nuvera Model II - RV9,, Nuvera Model III - RV10,,and Nuvera Model IV - RV11.

The Software Update Manager has the ability to download software updates and patches from the Xerox Download Server and install them on top of a previously-installed FFPS software release. The Software Update Manager will only display updates that are appropriate for the current FFPS release and printer product.

This document has procedures to:

1. Setup the FFPS system to provide Software Update Manager with access to the Xerox Download Manager Server.

2. Download and install the Security patch from the Xerox Download Manager server.

Note: because the procedures described will be executed by the user while having ultimate System Administration privileges (aka root password mode), it is critical that the commands be entered exactly as noted. Otherwise it is possible to modify the Operating System or the FFPS software in ways that are unintended and could result in the system being unusable or unstable. Xerox is not responsible for any mistakes made by the user in attempting these procedures. If there is any uncertainty about how to perform these procedures, please request help or advice from your local Xerox Service representative.

Pre-requisites:

To use the FFPS Software Update Manager, the Customer will need:

1. An active FFPS login account which is associated with the FFPS System Administrator group.

2. The “root” password for the Solaris Operating System; if the System Administrator does not have this, you may need to confirm with your IT department or your local Xerox Customer Service Engineer.

3. The Xerox “Product Serial Number”, which is associated with the Print Engine hardware device.

4. If the Customer’s network has an HTTP (Web) Proxy Server (or Firewall), then you will need to know the network (IP) address of the Proxy Server device and the Port Number to be used by FFPS to access the Proxy Server.

5. Physical access to the FFPS Graphical User Interface (monitor), keyboard, and mouse is required. The Software Update Manager cannot be run remotely.

Be prepared to re-boot the FFPS DFE after the patch has been downloaded. This requires knowledge of the Operational procedures required to “Pause the Printer” and if necessary, “Hold” any active jobs.

3.0 Network Proxy Setup for Access to the Xerox Update/Patch Server

Most customer networks use a HTTP Proxy or firewall to restrict access to the Internet. Because of this, the System Administrator for FFPS will need to configure the FFPS Software Update Manager to know about the customer's Proxy Server network (IP) address, and Port number.

Note: The FFPS Security profile must be set to 'Low' to use the Software Update Manager. The Software Update Manager is not able to access the Xerox Update/Patch server when the FFPS Security Profile is defined as 'High'. Therefore, if the FFPS system is running with the Security Profile set to 'High', be sure to change this setting to 'Low' to download the Security patch using Software Update Manager. Typically a patch update is installed with the Security profile remaining at 'Low'. Then, the Security Profile can be changed back to 'High' after the install has been completed. As an option, the Security profile could be set back to 'High' after the patch update has been downloaded. Later, the patch can be installed when the Security Profile is set to 'High.

Configuring the HTTP Proxy Settings on FFPS v8 and v9:

Set the Proxy Information on the FFPS system using the procedures below. Refer to the illustration for an example of what the display will show.

Note: *The proxy setup described below is only available in the FFPS GUI for FFPS v8 and v9 software releases. An alternative method to setup the proxy information for FFPS v7 must be performed in a terminal window. This is described in the section which follows this one.*

1. If necessary, Login to the FFPS GUI with an account that has System Administrator rights.

2. Looking at the Menu Bar, click on the word 'Setup'. Then, click on the menu item: Network Configuration'.

3. Next, click on the 'Options' Tab. The window will show a button labeled 'Proxy Configuration Settings'. Click on that button and a popup window is displayed.

4. Input the network (IP) address of the customer's Proxy Server and the Port number. Then click on Apply.

Configuring the HTTP Proxy Settings on FFPS v7:

The HTTP Proxy settings can be configured at the Solaris (Unix) command windows. This is done as follows:

1. Log into a terminal window as FFPS system administrator. Enter the "su" command and enter the 'root' password. At this point the command prompt displayed should be the "hash sign" (**#**). This indicates the system is at the "root prompt", and waiting to be given a system-level command.

In the following steps, do not enter the # sign again. It may be shown in the example to indicate the command is being entered at the # prompt.

2. Enter this string: cd /opt/XRXnps/bin

    - Note there is a space character between 'cd' and the forward-slash symbol

3. Enter the command ‘setupUpdateConfigProxy’, followed by the proxy information. Here is the format of this command: ./setupUpdateConfigProxy <HTTP Proxy Server IP Address or Domain> <HTTP Proxy Server Port>

   - Notice the command must be prefaced with a leading period character followed by a forward-slash symbol.

   - The “less than/greater than” brackets are not entered; they illustrate where the two data values are to be entered, and there is a space before and after the values.

   Example:

   # ./setUpdateConfigProxy www.company.com 4000
   Successfully setting Proxy IP: www.company.com, and Proxy Port: 4000
   #

4.0 Download & Install Shellshock Patch for X86

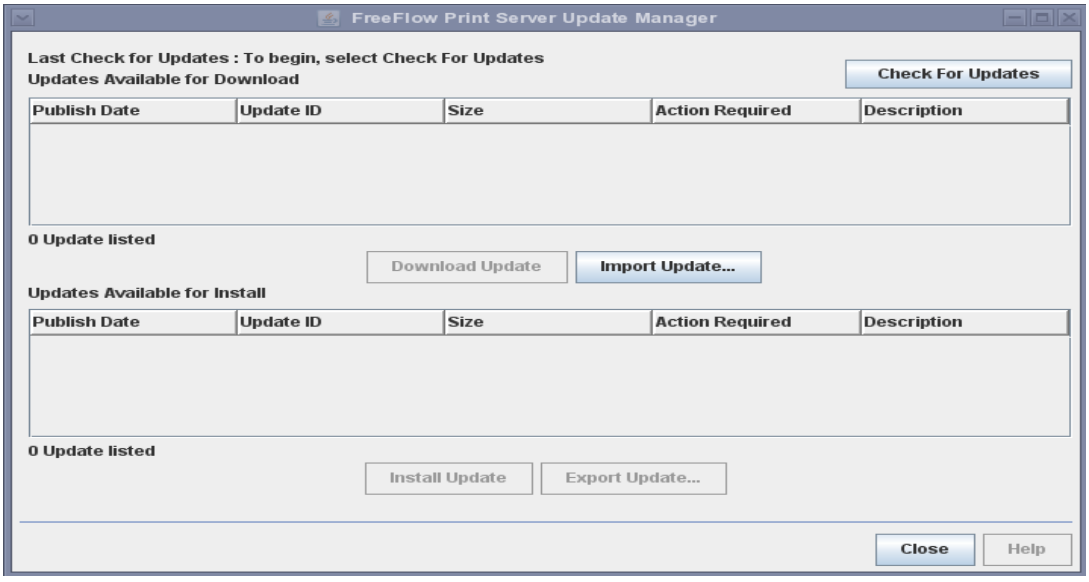
Download and install the Patch using FFPS Software Update Manager (UM) with the procedures below:

Start Update Manager:

For FFPS v8 and v9 releases, the Update Manager can be launched via the "Launch…" menu.

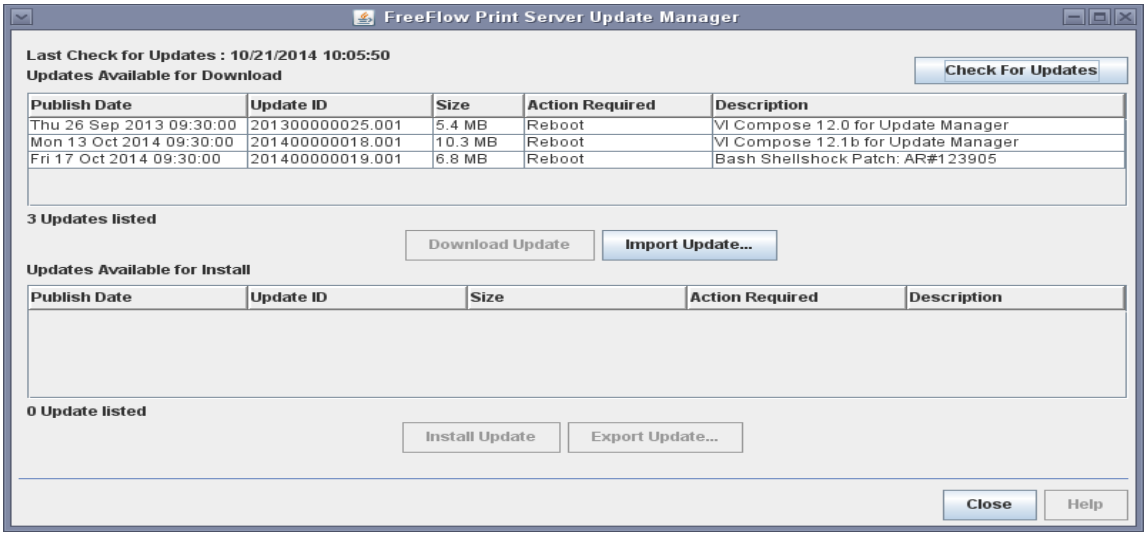
For FFPS v7 (and also v8 and v9), the Update Manager is launched by using a Unix Terminal (Command) Window as follows:

1. Open a Unix terminal (command) window
2. Log into the terminal window as FFPS system administrator, and enter the "su" command. Followed by the "enter" key Then enter the root password, and the "enter" key.
3. Enter the following commands to start the FFPS Update Manager:
   a. cd /opt/XRXnps/bin
   b. If your software is FFPS v7, enter: ./UpdateClientstart.sh
   c. If your software is FFPS v8 or v9, enter: ./UpdateManager.sh
   d. You should see the following GUI screen on FFPS v7. On FFPS v8 and v9, the screen may appear somewhat different but the buttons and functions are the same:



Check for Updates:

1. Select the 'Check for Updates' button in the upper right corner of the Update Manager UI. This will list one or more patches as illustrated below:

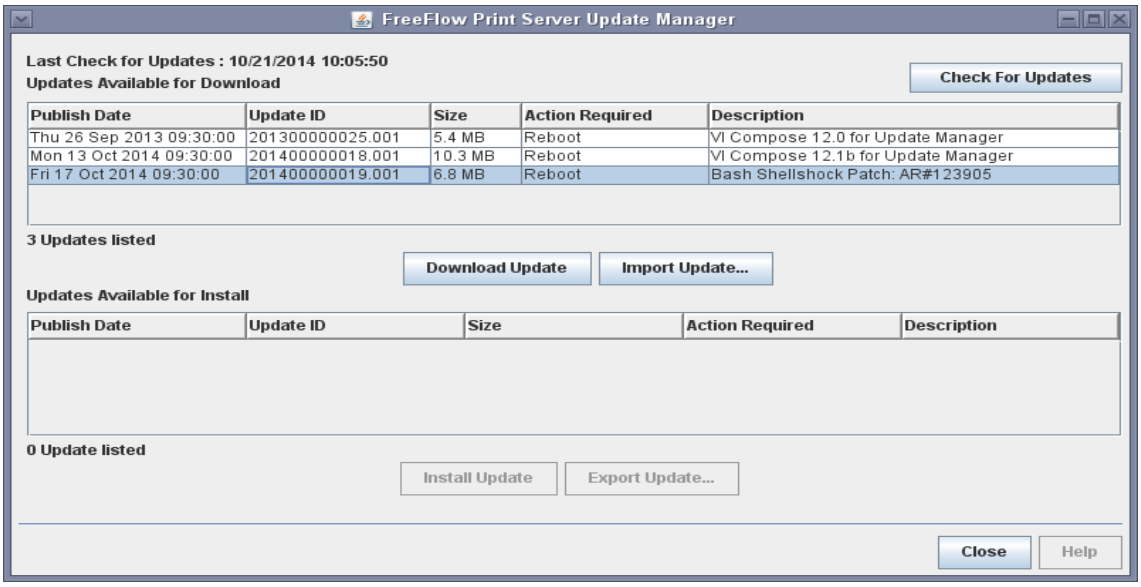


NOTE: At this point, you may see a message in a Dialog Box indicating you need to update the Update Manager, before you can proceed to see the available patches/updates for your system. It is recommended to accept the choice to download and install the newer version. If you choose not to do so, the Software Update Manager may not be able to access the Bash Patch.

Select the Bash Patch:

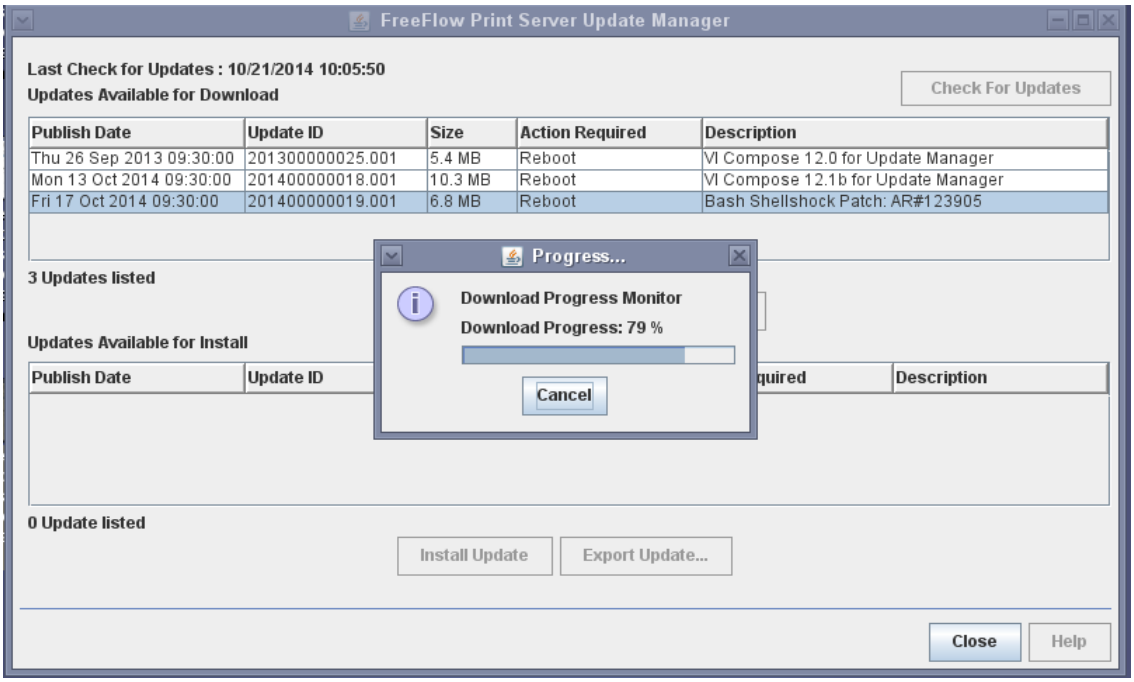
2. In the FFPS Update Manager UI under 'Updates Available for Download', highlight the record:

   - ✓ **Update ID:** 201400000019.001: '**Bash Shellshock Patch: AR#123905**'
   - ✓ Instead of Column Heading of **"Update ID",** you may see **"Version"**. The other values should be the same.

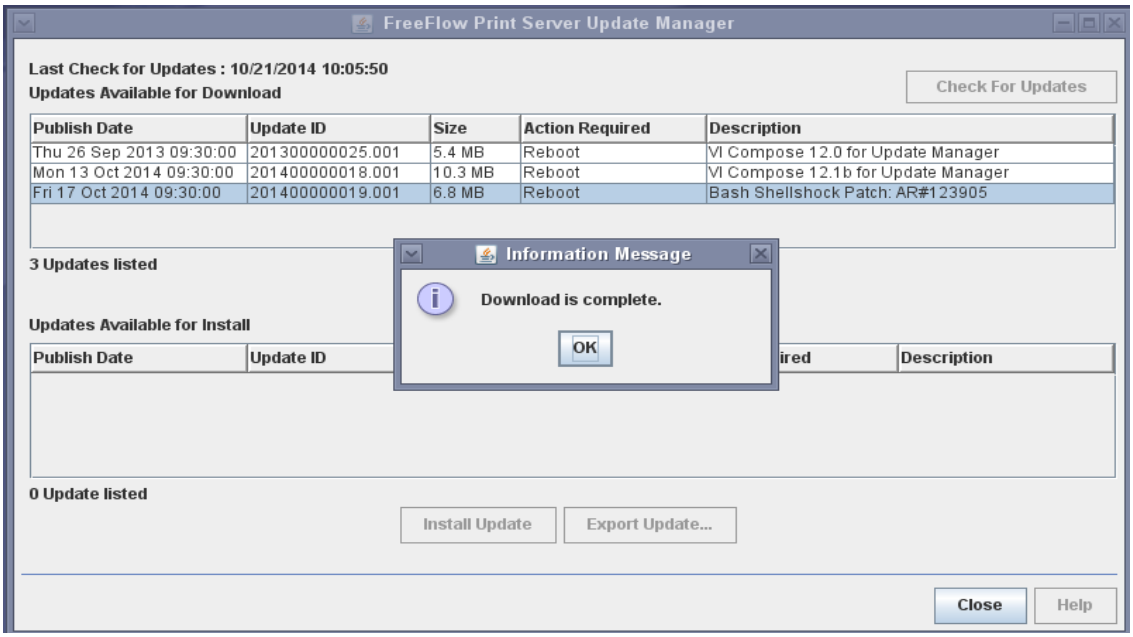


Download the Patch:

3. Select the 'Download Update' button and follow prompts to initiate the patch download. The Download progress will be displayed as illustrated below:



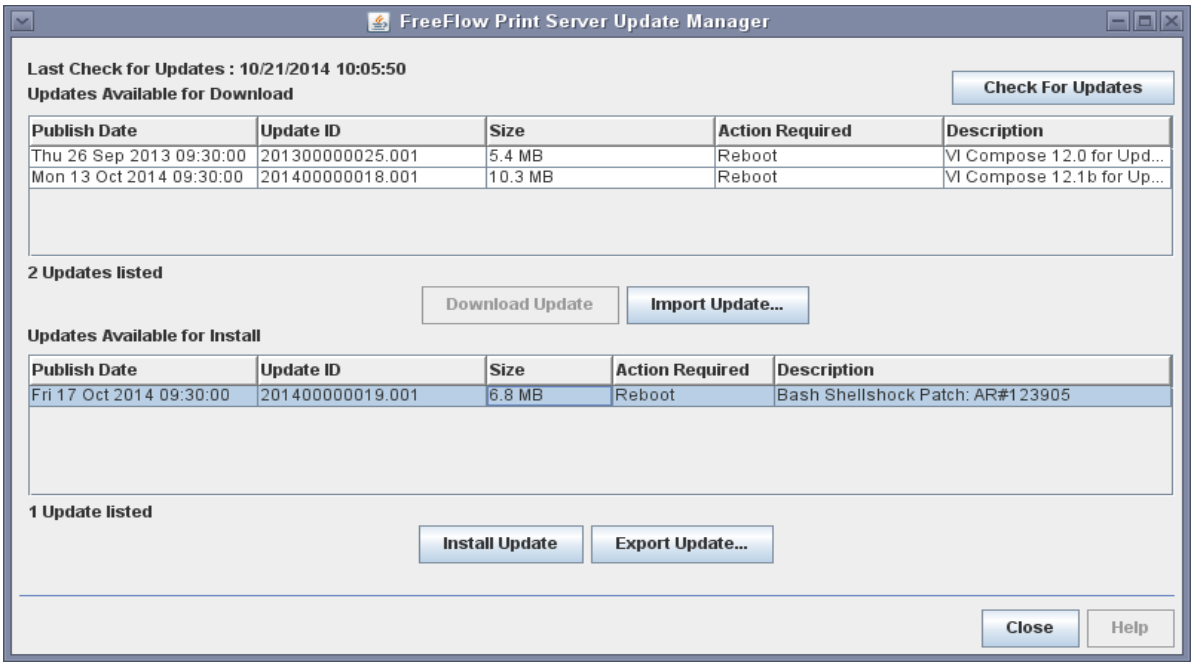
4. Once the download is completed, select the 'OK" button that is illustrated below:



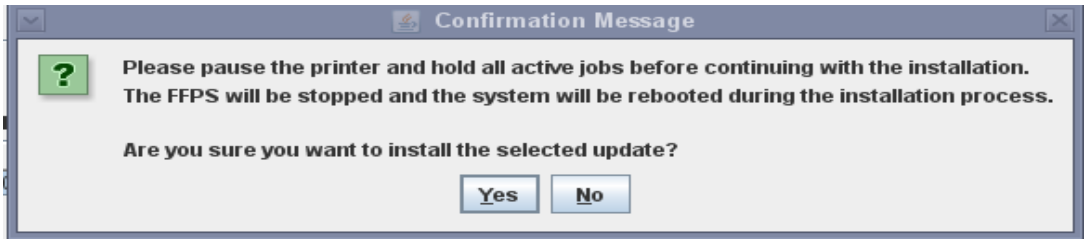
Install the Patch:

5. Note: Installation of the Bash Patch will require a re-boot of the FFPS DFE. For this reason, you will need to Pause the printer and Hold any active jobs in the FFPS Job Manager UI before installing the Patch.

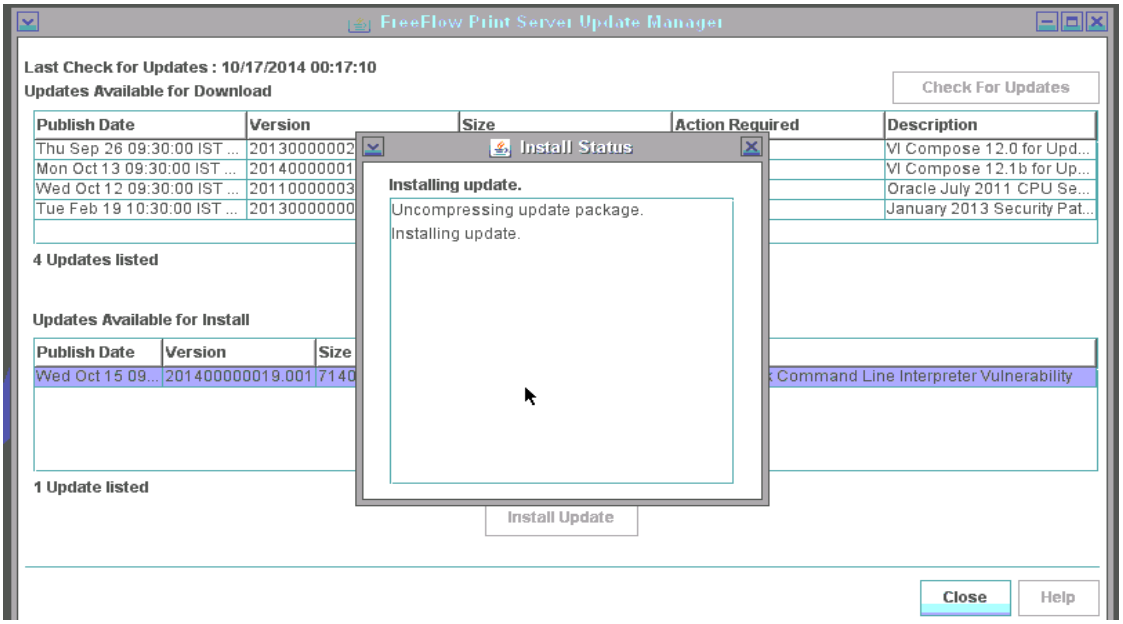
6. Highlight 201400000019.001 under 'Updates Available for Install ' section of the FFPS UM UI, and then select the 'Install Update' option illustrated below:



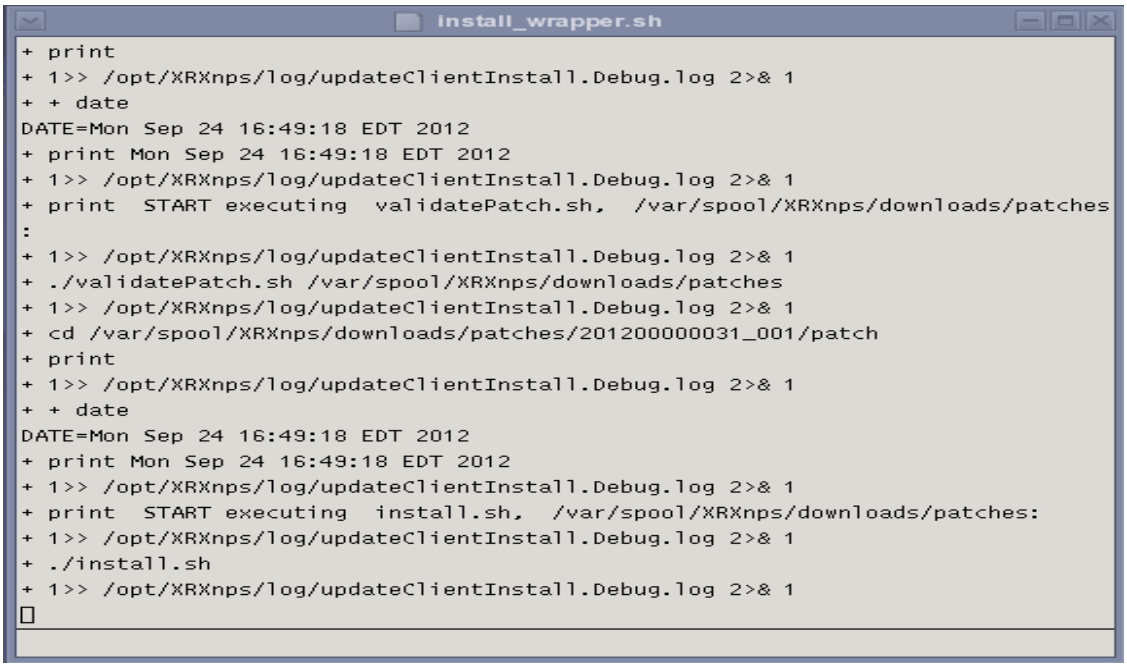
7. Pause the printer and hold any active jobs in the FFPS Job Manager UI before installing the Security Patch Cluster. Select the 'Yes' option to the Confirmation Message question that is illustrated below:



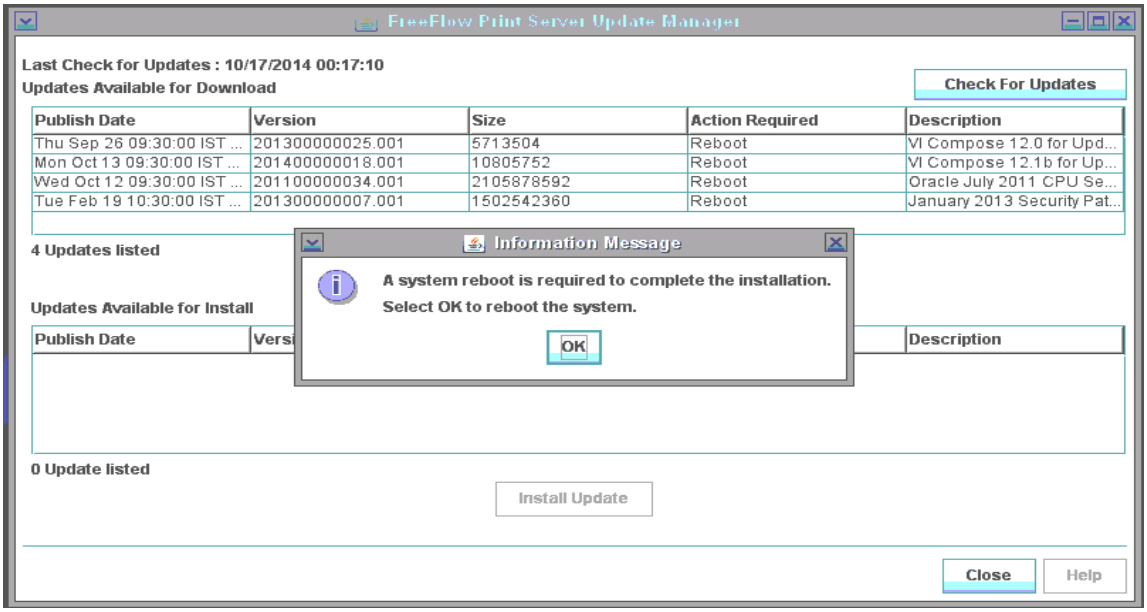
8. This will begin the installation of the FFPS Security patch cluster as illustrated below:



9. As the Security patch is installed an informational dialog window is displayed showing logging activity. See the example illustrated below:



10. Once the Patch install has been completed select the 'OK' button from the 'Update is Complete' informational dialog window illustrated below:



The Solaris / FFPS system will automatically reboot and initialize into "single-user mode". You will see Security patch add messages scroll up the screen indicating specific patches are being installed. Once all patches have been installed another automatic reboot of the system will occur. The Solaris OS, Gnome Desktop and FFPS software will initialize and the system should become ready for job processing and printing.

Nuvera NOTE: The Nuvera printer will power off after the Patch has been successfully installed. The User will need to power-up the printer after the Security patches have been installed to initialize the system to be ready for job processing and printing.

NOTE: The Update Manager log (updateClientInstall.Debug.log) is captured in the /opt/XRXnps/log directory. If there are any problems with the Security Patch Installation process, the user may be requested to deliver this log file to the FFPS 2nd-Level support team for analysis and further action.

5.0 Verify whether the patch is installed on the system

To confirm patch is loaded, log into a terminal window as FFPS system administrator. Enter the “su” command and enter the ‘root’ password. At this point the command prompt displayed should be the “hash sign” (#). This indicates the system is at the “root prompt”, and waiting to be given a system-level command.

1. Enter the root password when prompted
2. Enter the following command: **patchadd –p | grep 126547-07**
3. Patch 126547-07 should be listed..