Xerox Security Bulletin XRX20-009

Xerox® FreeFlow® Print Server v7 / Solaris® 11

Supports: Xerox Nuvera® PSIP 14.0/14.1 Printer Products

Deliverable: April 2020 Security Patch Cluster
Includes: Java 7 Update 261
Bulletin Date: May 19, 2020

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements for the Solaris® Operating System platform. Oracle® does not provide these patches to the public but authorize vendors like Xerox® to deliver them to customers with an active FreeFlow® Print Server Support Contracts (FSMA). Customers who may have an Oracle® Support Contract for their non-FreeFlow® Print Server / Solaris® Servers should not install patches not prepared/delivered by Xerox®. Installing non-authorized patches for the FreeFlow® Print Server software violates Oracle® agreements, can render the platform inoperable, and result in downtime and/or a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **April 2020 Security Patch Cluster**
   - Supersedes January 2020 Security Patch Cluster
   - October 2017 Security Patch Cluster install is prerequisite.
   - October 2018 Security Patch Cluster install is prerequisite.
2. **Java 7 Update 261 Software**
   - Supersedes Java 7 Update 251 Software
3. **Firefox 52.9.0 Software**
   - Same version delivered with January 2020 Security Patch Cluster.

Caveat: If the April 2018 Security Patch Cluster (or newer version) is not installed, inserting a USB drive into the USB port on the FreeFlow® Print Server will result in a keyboard and mouse freeze up, and make them inoperable. The April 2018 Security Patch Cluster (or newer version) includes patches to fix this issue. If the April 2018 Security Patch Cluster (or newer version) is not installed, we recommend transferring the Security Patch Cluster files to the FreeFlow® Print Server hard disk over an SFTP connection and installing from the hard disk. This method can be used to overcome the USB issues.

See US-CERT Common Vulnerability Exposures (CVE) the April 2020 Security Patch Cluster remediate in table below:

April 2020 Security Patch Cluster Remediated US-CERT CVE's			
CVE-2020-1935	CVE-2020-2851	CVE-2020-2944	CVE-2019-17563
CVE-2020-1938	CVE-2020-2927	CVE-2019-12418	CVE-2019-17569

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 261 software below:

Java 7 Update 261 Software Remediated US-CERT CVE's			
CVE-2020-2773	CVE-2020-2757	CVE-2020-2800	CVE-2020-2805
CVE-2020-2756	CVE-2020-2781	CVE-2020-2803	CVE-2020-2830

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v52.9.0 software below:

Firefox v52.9.0 Software Remediated US-CERT CVE's					
CVE-2018-12359	CVE-2018-12364	CVE-2018-5150	CVE-2018-5157	CVE-2018-5174	CVE-2018-6126
CVE-2018-12360	CVE-2018-12365	CVE-2018-5154	CVE-2018-5158	CVE-2018-5178	
CVE-2018-12362	CVE-2018-12366	CVE-2018-5155	CVE-2018-5159	CVE-2018-5183	
CVE-2018-12363	CVE-2018-12368	CVE-2018-5156	CVE-2018-5168	CVE-2018-5188	

Note: Xerox® recommends that customers evaluate their security needs periodically and if they need Security patches to address the above CVE issues, schedule an activity with their Xerox Service team to install this announced Security Patch Cluster. Alternatively, the customer can install the Security Patch Cluster using the Update Manager UI from the Xerox® FreeFlow® Print Server Platform.

2.0 Applicability

The customer can schedule a Xerox Service or Analyst representative to deliver and install the Security Patch Cluster from USB/DVD media or the hard disk on the FreeFlow® Print Server platform. A customer can work with the Xerox CSE/Analyst to install the quarterly Security Patch Clusters if they have the expertise. The Xerox CSE/Analyst would be required to provide the Security Patch Cluster deliverables if they agree to allow their customer install.

The April 2020 Security Patch Cluster is available for the FreeFlow® Print Server v7 release on the Solaris® 11.3 OS for the Xerox® printer products below:

1. Nuvera® 100/120/144/157 EA Digital Production System
2. Nuvera® 200/288/314 EA Perfecting Production System
3. Nuvera® 100/120/144 MX Digital Production System
4. Nuvera® 200/288 MX Perfecting Production System

This Security patch deliverable has been tested on the FreeFlow® Print Server 73.I1.10.11 and 73.I4.44A.S11 software releases. We have not tested the April 2020 Security Patch Cluster on all earlier FreeFlow® Print Server 7.3 releases, but there should not be any problems on these releases.

It is a prerequisite to install the October 2017 and October 2018 Security Patch Clusters on the FreeFlow® Print Server platform before installing the April 2020 Security Patch Cluster. A patch version script is provided to assist with identification of the current Security Patch Cluster version installed and another version information (E.g., Solaris® OS, Firefox, etc.). If the script output illustrates the October 2018 Security Patch Cluster (or newer version) is installed the prerequisite is satisfied.

The October 2017 and October 2018 Security Patch Clusters are too large to be supported by Update Manager. These larger deliverables can be transported to the customer location on DVD/USB media, or a laptop computer hard drive, and installed from a directory location on the FreeFlow Print Server platform. As a result of their large size, we deliver the October 2017 and October 2018 Security Patch Clusters as three-part ZIP files. They can be transferred to the FreeFlow Print Server over the network using SFTP or copied from DVD media to prepare for install. The April 2020 Security Patch Cluster is small enough for install using the Update Manager UI. However, the FreeFlow® Print Server application supported on Solaris® 11 is not yet supported for install from the Update Manager UI.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool that enables identification of the currently installed Solaris® OS version, FreeFlow® Print Server software version, Security Patch Cluster version, Java Software version. This tool can be initially run to determine if the prerequisite October 2018 Security Patch Cluster is currently installed. Example output from this script for the FreeFlow® Print Server v9 software is as follows:

Solaris® OS Version:	11.3
FFPS Release Version	7.0_SP-3_73.I4.44A
FFPS Release Version	7.0_SP-3_(73.I4.44A.11.86)
FFPS Patch Cluster	April 2020
Java Version	Java 7 Update 261
Base Repository	Installed
Firefox Version	52.9.0
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

The above versions are the correct information after installing the April 2020 Security Patch Cluster.

3.0 Patch Install

Xerox® strives to deliver critical Security patch updates in a timely manner. The customer process to obtain Security Patch Cluster updates (delivered on a quarterly basis) is to contact the Xerox hotline support number. Xerox Service or an analyst can install the Patch Cluster using a script utility that will support install from USB/DVD media, or from the hard disk on the FreeFlow® Print Server platform.

The Security Patch Cluster deliverables are available on a secure FTP site once they are ready for customer delivery. The Xerox CSE/Analyst can download and prepare for the install by writing the Security patch update into a known directory on the FreeFlow® Print Server platform, or on DVD/USB media. Delivery of the Security Patch Cluster includes an ISO and ZIP archive file for convenience. Once the patch cluster has been prepared on media, run the provided install script to perform the install. The install script accepts an argument that identifies the media that contains a copy of the FreeFlow® Print Server Security Patch Cluster. (e.g., # installSecPatches.sh [disk | usb | dvd]).

Delivery of the April 2020 Security Patch Cluster includes a ZIP and ISO image file. The ISO image file can be written to DVD media to transport and install on the FreeFlow® Print Server platform. The ZIP file can be copied to a well-defined location on the FreeFlow® Print Server hard drive to prepare for install. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install. Alternatively, the April 2020 Security Patch Cluster can be installed from USB/DVD media.

Note: The install of this Security Patch Cluster can fail if the archive file containing the software is corrupted from when downloading the deliverables from the SFTP site, copying them to USB media or uploading them to the hard drive on the FreeFlow® Print Server platform over a network connection. The table below illustrate file size on Windows®, file size on Solaris® and checksum on Solaris® for the April 2020 Security Patch Cluster files.

April 2020 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Apr2020AndJava7Update261Patches_v7S11.zip	2,215,638	2,268,813,040	60170 4431276
Apr2020AndJava7Update261Patches_v7S11.iso	2,215,988	2,269,171,712	23144 4431976

Verify integrity of the Security Patch files from the FreeFlow® Print Server hard drive by comparing it to the original archive file size checksum with the actual checksum of these files on the platform. Change directory to the location of the Security Patch Cluster file and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., sum **Apr2020AndJava7Update261Patches_v7S11.zip**). The output of the '**sum**' command should match the checksum in the above table.

4.0 Disclaimer

The information provided in this Xerox® Product Response is provided "as is" without warranty of any kind. Xerox® Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox® Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox® Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox® Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.