Xerox Security Bulletin XRX19-012

Xerox® FreeFlow® Print Server v8

For: Solaris® 10 Operating System
Install Method: DVD/USB Media

Deliverable: April 2019 Security Patch Cluster
Includes: Java 7 Update 211
Bulletin Date: May 20, 2019

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT Security vulnerabilities and reliability improvements for the Solaris Operating System. Oracle® does provide patches to the public but authorize vendors like Xerox® to deliver if there is an active FreeFlow® Print Server Support Contracts (FSMA). Customers that have an Oracle® Support Contract for their non-FreeFlow® Print Server Solaris Servers should only install patches prepared/delivered by Xerox®. Installing non-authorized patches for the FreeFlow® Print Server software violates Oracle® agreements, and 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 2019 Security Patch Cluster**
   - Supersedes the January 2019 Security Patch Cluster
2. **Java 6 Update 211 Software**
   - Same version included in pervious January 2019 Security Patch Cluster

See US-CERT Common Vulnerability Exposures (CVE's) mitigated by the April 2019 Security Patch Cluster below:

April 2019 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2016-1549	CVE-2018-0734	CVE-2018-0735	CVE-2018-5407	CVE-2018-7170	CVE-2018-20685

See the US-CERT Common Vulnerability Exposures (CVE's) mitigated by the Java 6 Update 211 Software table below:

Java 6 Update 211 Software Remediated US-CERT CVE's			
CVE-2018-3136	CVE-2018-3149	CVE-2018-3180	CVE-2018-13785
CVE-2018-3139	CVE-2018-3169	CVE-2018-3214	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v52.0.2 Software below:

Firefox v52.0.2 Software Remediated US-CERT CVE's					
CVE-2015-0820	CVE-2016-2836	CVE-2016-5255	CVE-2016-5266	CVE-2016-5277	CVE-2016-5279
CVE-2015-4481	CVE-2016-2837	CVE-2016-5258	CVE-2016-5267	CVE-2016-5280	CVE-2016-5282
CVE-2015-4508	CVE-2016-2838	CVE-2016-5259	CVE-2016-5268	CVE-2016-5281	CVE-2016-5283
CVE-2016-2832	CVE-2016-2839	CVE-2016-5260	CVE-2016-5256	CVE-2016-2827	CVE-2016-5284
CVE-2016-2833	CVE-2016-5250	CVE-2016-5262	CVE-2016-5257	CVE-2016-5271	
CVE-2016-5254	CVE-2016-5251	CVE-2016-5263	CVE-2016-5270	CVE-2016-5272	
CVE-2016-5261	CVE-2016-5252	CVE-2016-5264	CVE-2016-5274	CVE-2016-5275	
CVE-2016-2835	CVE-2016-5253	CVE-2016-5265	CVE-2016-5276	CVE-2016-5278	

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 using media (DVD/USB). A customer can only perform the install procedures with approval of the Xerox CSE/Analyst. Xerox® offers an electronic delivery for "easy to use" install of a Security Patch Cluster, which is more suited for a customer to manage the quarterly patches on their own.

This Security patch deliverable has been tested on the FreeFlow® Print Server 82.I2.15 software releases. We have not tested the April 2019 Security Patch Cluster on all earlier FreeFlow® Print Server 8.2 releases, but there should not be any problems on these releases. It is always good practice to create a System Backup before installing the Security patches.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool (accessible from a secure FTP site) that enables identification of the currently installed FreeFlow® Print Server software release, Security Patch Cluster, and Java Software version. Run this tool after the Security Patch Cluster install to validate a successful install. Example output from this script for the FreeFlow® Print Server v8 software release is as following:

Solaris OS Version	10 Update 11
FFPS Release Version	8.0-2_SP-2_82.I2.15
FFPS Patch Cluster	April 2019
Java Version	Java 6 Update 211

The April 2019 Security Patch Cluster is available for the FreeFlow® Print Server v8 release running on the Xerox® printer products below:

1. Xerox® iGen®4 Press
2. Xerox® Color 800/1000 Press
3. Xerox® Color 560/570 Printer
4. Xerox ® 700/700i Digital Color Press
5. Xerox ® 770 Digital Color Press

CAVEAT: We have a caveat with the April 2019 Security Patch Cluster for the FreeFlow® Print Server 8.2 software release. The FreeFlow Print Server application is not able to access remote SMB shares after installing the April 2019 Security Patch Cluster. This does not affect the SMB shares used for Hot Folder workflow. The affected capabilities are SMB access of remote job files by the 'Print From File' client, and storing PDF/TIFF files to a remote location over SMB from a hardcopy scan (E.g., commonly done on a Nuvera printer). It is not common for a Security conscience customer to use SMB workflows, so this should not affect many customers.

3.0 Patch Install

Xerox® strives to deliver these 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 installing the patch cluster from the FreeFlow® Print Server hard disk, DVD, or USB media.

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 [diskl dvdl usb]).

Important: The install of this Security patch update can fail if the archive file containing the patches is corrupted from file transfer or writing to DVD media. There have been reported install failures when the archive file written on DVD media was corrupt. Writing to media using some DVD write applications and media types could result in a corrupted Security Patch Cluster. The tables below illustrate Solaris checksums and file size on Windows for the Security Patch Cluster ZIP and ISO files. We provide these numbers in this bulletin as a reference to check against the actual checksum. The file size and check sum of these files on Windows and Solaris are as follows:

FreeFlow® Print Server v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Apr2019AndJava6U211Patches_v8.zip	2,238,203	2,291,919,569	45251 4476406
Apr2019AndJava6U211Patches_v8.iso	2,238,554	2,292,279,296	6288 4477108

Verify the **Apr2019AndJava6U211Patches_v8.zip** file contained on the DVD/USB media or hard drive by comparing it to the original archive file size and checksum in the above table. Change directory to the file location (DVD, USB, or hard disk) and type "**sum Apr2019AndJava6U211Patches_v8.zip"** from a terminal window. The checksum value should be "**45251 4476406**", and can be used to validate the correct April 2019 Security Patch Cluster on the DVD/USB or the hard drive.

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.