Xerox Security Bulletin XRX18-005
Xerox® FreeFlow® Print Server v8

Media Delivery (DVD/USB) of: January 2018 Security Patch Cluster
Includes: Java 6 Update 181
Bulletin Date: February 19, 2018

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Solaris Operating platform. Oracle® does not provide these patches to the public, but authorize vendors like Xerox® to deliver them to Customers with 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. **January 2018 Security Patch Cluster**
   - This supersedes the October 2017 Security Patch Cluster
2. **Java 6 Update 181 Software**
   - This supersedes Java 6 Update 171 Software

CAVEAT: We have a caveat with the January 2018 Security Patch Cluster for the FreeFlow® Print Server 8.2 software releases. The FreeFlow Print Server application is not able to access remote SMB shares after installing the January 2018 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.

See US-CERT Common Vulnerability Exposures (CVE) the January 2018 Security Patch Cluster remediate in table below:

January 2018 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2011-2391	CVE-2016-0701	CVE-2017-1000083	CVE-2017-12163	CVE-2017-3736	CVE-2018-2710
CVE-2015-3193	CVE-2016-5824	CVE-2017-12150	CVE-2017-14989	CVE-2017-3737	
CVE-2015-7674	CVE-2016-9584	CVE-2017-12151	CVE-2017-3732	CVE-2017-3738	

See the US-CERT Common Vulnerability Exposures (CVE) the Java 6 Update 181 Software remediate in table below:

Java 6 Update 181 Software CVE Remediated US-CERT CVE's				
CVE-2018-2579	CVE-2018-2602	CVE-2018-2629	CVE-2018-2637	CVE-2018-2663
CVE-2018-2588	CVE-2018-2603	CVE-2018-2633	CVE-2018-2641	CVE-2018-2677
CVE-2018-2599	CVE-2018-2618	CVE-2018-2634	CVE-2018-2657	CVE-2018-2678

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® does offer an electronic delivery and "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.H3.64 software release. We have not tested the January 2018 Security Patch Cluster on all earlier FreeFlow® Print Server 8.2 releases, but there should not be any problems on these releases.

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:

FFPS Release Version		8.0-2_SP-2_(82.H3.64.86)
FFPS Patch Cluster		January 2018
Java Version		Java 6 Update 181

The January 2018 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

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]).

< Continued on Next Page >

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
Jan2018AndJava6U171Patches_v8.zip	2,098,731	2,149,100,077	42957 4197462
Jan2018AndJava6U171Patches_v8.iso	2,099,082	2,149,459,968	4849 4198164

Verify the **Jan2018AndJava6U171Patches_v8.zip** file contained on the DVD media by comparing it to the original archive file size and checksum. Copy this file to a location on the FreeFlow® Print Server platform and type '**sum Jan2018AndJava6U171Patches_v8.zip'** from a terminal window. The checksum value should be **'43957 4197462'**, and can be used to validate the correct January 2018 Security Patch Cluster on the DVD/USB.

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.

© 2018 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, iGen®, and FreeFlow® are trademarks of Xerox Corporation in the United States and/or other countries. BR21127
Other company trademarks are also acknowledged