Xerox Security Bulletin XRX17-028
Xerox® FreeFlow® Print Server v8

Media Delivery (DVD/USB) of: October 2017 Security Patch Cluster
Includes: Java 6 Update 171
Bulletin Date: December 4, 2017

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. **October 2017 Security Patch Cluster**
   - This supersedes the July 2016 Security Patch Cluster
2. **Java 6 Update 171 Software**
   - This supersedes Java 6 Update 161 Software

CAVEAT: We have a caveat with the October 2017 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 October 2017 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 October 2017 Security Patch Cluster remediate in table below:

October 2017 Security Patch Cluster CVE Remediated US-CERT CVE's					
CVE-2016-1238	CVE-2017-6452	CVE-2017-7186	CVE-2017-8343	CVE-2017-8351	CVE-2017-8779
CVE-2016-9042	CVE-2017-6455	CVE-2017-7244	CVE-2017-8344	CVE-2017-8352	CVE-2017-8786
CVE-2017-11103	CVE-2017-6458	CVE-2017-7245	CVE-2017-8345	CVE-2017-8353	CVE-2017-8804
CVE-2017-3167	CVE-2017-6459	CVE-2017-7246	CVE-2017-8346	CVE-2017-8354	CVE-2017-8830
CVE-2017-3169	CVE-2017-6460	CVE-2017-7619	CVE-2017-8347	CVE-2017-8355	CVE-2017-9098
CVE-2017-3629	CVE-2017-6462	CVE-2017-7659	CVE-2017-8348	CVE-2017-8356	CVE-2017-9788
CVE-2017-5664	CVE-2017-6463	CVE-2017-7668	CVE-2017-8349	CVE-2017-8357	CVE-2017-9789
CVE-2017-6451	CVE-2017-6464	CVE-2017-7679	CVE-2017-8350	CVE-2017-8765	

See the US-CERT Common Vulnerability Exposures (CVE) the Java 6 Update 171 Software remediate in table below:

Java 6 Update 171 Software CVE Remediated US-CERT CVE's					
CVE-2016-10165	CVE-2017-10281	CVE-2017-10295	CVE-2017-10349	CVE-2017-10347	CVE-2017-10357
CVE-2016-9841	CVE-2017-10285	CVE-2017-10345	CVE-2017-10350	CVE-2017-10348	CVE-2017-10388
CVE-2017-10274	CVE-2017-10293	CVE-2017-10346	CVE-2017-10355	CVE-2017-10356	

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 Security Patch Clusters, which is more suited for a customer to manage the quarterly patches on their own.

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_(81.G3.03.86)
FFPS Patch Cluster	October 2017
Java Version	Java 6 Update 171

The October 2017 Security Patch Cluster is available for the FreeFlow® Print Server Software Releases below:

FreeFlow® Print Server v8

Xerox® printer products running the FreeFlow® Print Server 81.G3.03 software release for:

- Xerox® iGen®4 Press
- Xerox® Color 800/1000 Press
- Xerox® Color 560/570 Printer
- Xerox ® 700/700i Digital Color Press
- Xerox ® 770 Digital Color Press

All previous FreeFlow® Print Server v8.2 software releases have not been tested with October 2017 Security Patch Cluster, but there should not be any problems on previous FreeFlow® Print Server 8.2 releases.

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 [disk| dvd| 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
Oct2017AndJava6U171Patches_v8.zip	2,098,731	2,149,100,077	42957 4197462
Oct2017AndJava6U171Patches_v8.iso	2,099,082	2,149,459,968	4849 4198164

Verify the Oct2017AndJava6U171Patches_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 Oct2017AndJava6U171Patches_v8.zip’ from a terminal window. The checksum value should be ‘43957 4197462’, and can be used to validate the correct October 2017 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.