Xerox Security Bulletin XRX17-019

Xerox® FreeFlow® Print Server v8

Media Delivery (DVD/USB) of:
July 2017 Security Patch Cluster
Java 6 Update 161

Bulletin Date: August 10, 2017

A. 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. **July 2017 Security Patch Cluster**
   - This supersedes the April 2016 Security Patch Cluster
2. **Java 6 Update 161 Software**
   - This supersedes Java 6 Update 151 Software

See the US-CERT Common Vulnerability Exposures (CVE's) remediated by the July 2017 Security Patch Cluster illustrated below:

July 2017 Security Patch Cluster CVE Remediation Table					
CVE-2013-7447	CVE-2015-8875	CVE-2017-10003	CVE-2017-10036	CVE-2017-2619	CVE-2017-3630
CVE-2014-9766	CVE-2016-10164	CVE-2017-10004	CVE-2017-10042	CVE-2017-3622	CVE-2017-3632
CVE-2015-7674	CVE-2016-5384	CVE-2017-10122	CVE-2017-10062	CVE-2017-3629	CVE-2017-7494

See the US-CERT Common Vulnerability Exposures (CVE's) remediated by the Java 6 Update 161 software illustrated below:

July 2017 Security Patch Cluster CVE Remediation Table				
CVE-2017-10053	CVE-2017-10089	CVE-2017-10102	CVE-2017-10109	CVE-2017-10135
CVE-2017-10067	CVE-2017-10087	CVE-2017-10105	CVE-2017-10110	CVE-2017-10193
CVE-2017-10074	CVE-2017-10096	CVE-2017-10107	CVE-2017-10115	CVE-2017-10198
CVE-2017-10081	CVE-2017-10101	CVE-2017-10108	CVE-2017-10116	CVE-2017-10243

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.

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	July 2017
Java Version	Java 6 Update 161

The July 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:

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

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

B. 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
July2017AndJava6U161Patches_v8.zip	2,099,873	2,150,269,857	58940 4199746
July2017AndJava6U161Patches_v8.iso	2,100,224	2,150,629,376	19420 4200448

Verify the **July2017AndJava6U161Patches_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 July2017AndJava6U161Patches_v8.zip'** from a terminal window. The checksum value should be **'58940 4199746'**, and can be used to validate the correct July 2017 Security Patch Cluster on the DVD/USB.

C. 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.

© 2017 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. BR22140
Other company trademarks are also acknowledged