Xerox Security Bulletin XRX17-011

Xerox® FreeFlow® Print Server v7 and v9

Media Delivery (DVD/USB) of:
April 2017 Security Patch Cluster
Java 7 Update 141

Bulletin Date: May 30, 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. April 2017 Security Patch Cluster
   - This supersedes the January 2017 Security Patch Cluster
2. Java 7 Update 141 Software
   - This supersedes Java 7 Update 121 Software

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

April 2017 Security Patch Cluster CVE Remediation Table					
CVE-2012-2369	CVE-2013-6481	CVE-2014-8092	CVE-2016-7428	CVE-2016-8862	CVE-2017-3731
CVE-2012-3461	CVE-2013-6482	CVE-2015-3418	CVE-2016-7429	CVE-2016-9131	CVE-2017-3732
CVE-2012-6152	CVE-2013-6483	CVE-2016-0736	CVE-2016-7431	CVE-2016-9147	CVE-2017-5506
CVE-2013-0271	CVE-2013-6484	CVE-2016-10144	CVE-2016-7433	CVE-2016-9298	CVE-2017-5507
CVE-2013-0272	CVE-2013-6485	CVE-2016-10145	CVE-2016-7434	CVE-2016-9310	CVE-2017-5508
CVE-2013-0273	CVE-2013-6486	CVE-2016-10146	CVE-2016-7799	CVE-2016-9311	CVE-2017-5509
CVE-2013-0274	CVE-2013-6487	CVE-2016-2161	CVE-2016-7906	CVE-2016-9312	CVE-2017-5510
CVE-2013-6477	CVE-2013-6489	CVE-2016-7055	CVE-2016-8707	CVE-2016-9444	CVE-2017-5511
CVE-2013-6478	CVE-2013-6490	CVE-2016-7426	CVE-2016-8740	CVE-2016-9556	
CVE-2013-6479	CVE-2014-0020	CVE-2016-7427	CVE-2016-8743	CVE-2016-9559	

See the US-CERT Common Vulnerability Exposures (CVE's) remediated by the Java 7 Update 141 Software illustrated below:

Java 7 Update 141 Software CVE Remediation Table			
CVE-2017-3509	CVE-2017-3512	CVE-2017-3526	CVE-2017-3539
CVE-2017-3511	CVE-2017-3514	CVE-2017-3533	CVE-2017-3544

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.

B. 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 CFO Web 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 v9 software release is as following:

FFPS Release Version	9.0_SP-3 (93.G4.74A)
FFPS Patch Cluster	April 2017
Java Version	Java 7 Update 141

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

FreeFlow® Print Server v7

Xerox printer products running the FreeFlow® Print Server 73.H0.23 software release for the:

1. Xerox Nuvera® 100/120/144/157 EA Digital Production System
2. Xerox Nuvera® 200/288/314 EA Perfecting Production System
3. Xerox Nuvera® 100/120/144 MX Digital Production System
4. Xerox Nuvera® 200/288 MX Perfecting Production System
5. Xerox® DocuPrint 100/115/135/155/180 MX Enterprise Printing System
6. Xerox® DocuTech® 6128/6155/6180 Production Publisher
7. Xerox® DocuTech® Highlight Color 128/155/180 Production Publisher
8. Xerox® DocuColor® 242/252/260/700,
9. Xerox® DocuColor® 5000AP
10. Xerox® DocuColor® 7002/8002
11. Xerox® DocuColor® 8080
12. Xerox® Digital Printer 4112/4127 Enterprise Printing System
13. Xerox® Digital 4590/4595 Copier/Printer

All previous FreeFlow® Print Server v7.3 software releases have not been tested with April 2017 Security Patch Cluster, but there should not be any problems on previous FreeFlow® Print Server 7.3 releases.

FreeFlow® Print Server v9

Xerox printer products running the FreeFlow® Print Server 93.G4.74A software release for:

1. Xerox® iGen® Products (iGen4, iGen150, Xerox® Color 8250 Presses)
2. Xerox® Versant 80/2100 Presses
3. Xerox® Color 800/100, 800i/1000i Presses
4. Xerox® Color Press J75/C75 Presses
5. Xerox® Color Press 560/570
6. Xerox® Impika® Compact Inkjet Press
7. Xerox® CiPress® 325/500 Production Inkjet System

8. Xerox® Rialto® 900 Inkjet Press
9. Xerox® D95/110/125/136 D95/110/125/136 Copier/Printers

All previous FreeFlow® Print Server v9.3 software releases have not been tested with April 2017 Security Patch Cluster, but there should not be any problems on previous FreeFlow® Print Server 9.3 releases.

C. 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 the CFO Web 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 v7

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Apr2017AndJava7U141Patches_v7.zip	2,167,026	2,219,106,649	47286 4334193
Apr2017AndJava7U141Patches_v7.iso	2,167,376	2,219,466,752	8362 4334896

Verify the **Apr2017AndJava7U141Patches_v7.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 Apr2017AndJava7U141Patches_v7.zip'** from a terminal window. The checksum value should be **'47286 4334193**, and can be used to validate the correct April 2017 Security Patch Cluster on the DVD/USB.

FreeFlow® Print Server v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Apr2017AndJava7U141Patches_v9.zip	2,378,828	2,435,919,704	26361 4757656
Apr2017AndJava7U141Patches_v9.iso	2,379,178	2,436,278,272	53285 4758356

Verify the **Apr2017AndJava7U141Patches_v9.zip** file contained on the DVD media by comparing it to the original archive file size and checksum. Copy this archive to a location on the FreeFlow® Print Server platform and type '**sum Apr2017AndJava7U141Patches_v9.zip**' from a terminal window. The checksum value should be '**26361 4757656'**, and can be used to validate the correct April 2017 Security Patch Cluster on the DVD/USB.

D. 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.