Xerox Security Bulletin XRX17-001

Xerox® FreeFlow® Print Server v7 and v9

Media Delivery (DVD/USB) of:
January 2017 Security Patch Cluster
Java 7 Update 121

Bulletin Date: February 15, 2017

Background

Oracle delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Solaris Operating System. 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-Free Flow Print Server Solaris Servers should not install patches not prepared/delivered by Xerox. Installing non-authorized patches for the Free Flow Print Server software violates Oracle agreements, can render the system inoperable, and result in downtime and/or a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **January 2017 Security Patch Cluster**
   - This supersedes the October 2016 Security Patch Cluster
2. **Java 7 Update 121 Software**
   - Same as included with the October 2016 Security Patch Cluster
   - This supersedes Java 7 Update 111 Software

This patch deliverable remediates the US-CERT announced Security vulnerabilities below:

CVE-2015-3228	CVE-2016-2335	CVE-2016-6302	CVE-2016-7101	CVE-2016-7522	CVE-2016-7532
CVE-2015-8957	CVE-2016-3465	CVE-2016-6303	CVE-2016-7513	CVE-2016-7523	CVE-2016-7533
CVE-2015-8958	CVE-2016-5384	CVE-2016-6304	CVE-2016-7514	CVE-2016-7524	CVE-2016-7534
CVE-2016-2177	CVE-2016-5542	CVE-2016-6305	CVE-2016-7515	CVE-2016-7525	CVE-2016-7535
CVE-2016-2178	CVE-2016-5554	CVE-2016-6306	CVE-2016-7516	CVE-2016-7526	CVE-2016-7536
CVE-2016-2179	CVE-2016-5556	CVE-2016-6307	CVE-2016-7517	CVE-2016-7527	CVE-2016-7537
CVE-2016-2180	CVE-2016-5568	CVE-2016-6308	CVE-2016-7518	CVE-2016-7528	CVE-2016-7538
CVE-2016-2181	CVE-2016-5573	CVE-2016-6309	CVE-2016-7519	CVE-2016-7529	CVE-2016-7539
CVE-2016-2182	CVE-2016-5582	CVE-2016-6823	CVE-2016-7520	CVE-2016-7530	CVE-2016-7540
CVE-2016-2183	CVE-2016-5597	CVE-2016-7052	CVE-2016-7521	CVE-2016-7531	CVE-2016-8864

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® Free Flow® Print Server Platform.

Applicability

The customer can schedule a Xerox Service or Analyst representative to deliver and install the Free Flow Print Server 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 Free Flow 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 Free Flow Print Server v9 software release is as following:

Free Flow Print Server Release Version	9.0_SP-3 (93.G3.74A)
Free Flow Print Server Patch Cluster	January 2017
Java Version	Java 7 Update 121

The January 2017 Security Patch Cluster is available for the Free Flow Print Server Software Releases below:

Free Flow Print Server v7

Xerox printer products running the Free Flow Print Server 73.G2.55 software release for the Free Flow Print Server 73.G2.55 for (Xerox Nuvera® 1XX EA Digital Production System (DPS) Series, 200/288/144/120/100, Xerox Nuvera® MX Digital Production System 200/288/314 EA), (Xerox® Enterprise Print System 1xx, Xerox® DocuTech® 61xx, 128/155/180 Highlight Color / Highlight Color Publisher), (Xerox® DocuColor® 242/252/260, 5000AP, 7002/8002, 8080, 700), (Xerox® Digital Printer 4112/4127, Xerox® Digital Copier/Printer 4590/4595) printers. All previous Free Flow Print Server v7.3 software releases have not been tested with January 2017 Security Patch Cluster, but there should not be any problems on previous Free Flow Print Server 7.3 releases.

Free Flow Print Server v9

Xerox printer products running the Free Flow Print Server 93.G4.74A software release for Xerox® iGen® Products (iGen4, iGen150 & Xerox® Color 8250), (Xerox® Versant 80/2100 Press, (Xerox® Color 800/100, Xerox® Color 800i/1000i) and Xerox® Color Press J75, XC C75, Xerox® Color Press 560/570 & Xerox® D95/110/125/136 D95/110/125/136 printers. All previous Free Flow Print Server v9.3 software releases have not been tested with January 2017 Security Patch Cluster, but there should not be any problems on previous Free Flow Print Server 9.3 releases.

Patch Install

Xerox strives to deliver these critical Security patch updates in a timely manner. The customer process to obtain Free Flow Print Server 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 Free Flow Print Server Security Patch Cluster using a script utility that will support installing the patch cluster from the Free Flow 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 Free Flow Print Server system, 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 Free Flow 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:

Free Flow Print Server v7

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Jan2017AndJava7U121Patches_v7.zip	2,136,857	2,188,140,924	8012 4273713
Jan2017AndJava7U121Patches_v7.iso	2,137,208	2,188,500,992	34135 4274416

Verify the **Jan2017AndJava7U121Patches_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 Free Flow Print Server system and type '**sum Jan2017AndJava7U121Patches_v7.zip'** from a terminal window. The checksum value should be **'8012 4273713'**, and can be used to validate the correct January 2017 Security Patch Cluster on the DVD/USB.

Free Flow Print Server v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Jan2017AndJava7U121Patches_v9.zip	2,219,018	2,272,274,112	62940 4438036
Jan2017AndJava7U121Patches_v9.iso	2,219,368	2,272,632,832	24056 4438736

Verify the **Jan2017AndJava7U121Patches_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 Free Flow Print Server system and type '**sum Jan2017AndJava7U121Patches_v9.zip**' from a terminal window. The checksum value should be '**62940 4438036'**, and can be used to validate the correct January 2017 Security Patch Cluster on the DVD/USB.

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.