



Xerox Security Bulletin XRX16-002 V1.0

FreeFlow Print Server v7, v8 and v9

Media Delivery (DVD/USB) of:

- October 2015 Security Patch Cluster (includes Java 6 Update 105)

01/13/2016

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 general public, but Xerox is authorized to deliver them to Customers with active FreeFlow Print Server (FFPS) Support Contracts (FSMA). Customers who may have an Oracle Support Contract for their non-FFPS Solaris Servers should not install patches that have not been customized by Xerox. Otherwise the FFPS software could be damaged and result in downtime and a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **October 2015 Security Patch Cluster**
 - ✓ This supersedes the July 2015 Security Patch Cluster
2. **Java 6 Update 105 Software**
 - ✓ This supersedes Java 6 Update 101 Software
3. **Supplement October 2015 Security Patch Cluster**
 - ✓ This updates the October 2015 Security Patch Cluster

The Security vulnerabilities that are remediated with this FFPS Security patch delivery are as follows:

CVE-2008-4770	CVE-2009-0696	CVE-2014-7185	CVE-2015-2642	CVE-2015-4734	CVE-2015-4803
CVE-2015-4805	CVE-2015-4806	CVE-2015-4835	CVE-2015-4842	CVE-2015-4843	CVE-2015-4844
CVE-2015-4860	CVE-2015-4869	CVE-2015-4872	CVE-2015-4881	CVE-2015-4882	CVE-2015-4883
CVE-2015-4893	CVE-2015-4902	CVE-2015-4903	CVE-2015-4911		

Supplement Security vulnerabilities remediated with this FFPS Security patch delivery are as follows:

CVE-2008-4316	CVE-2012-5668	CVE-2012-5669	CVE-2012-5670	CVE-2013-1788	CVE-2013-1789
CVE-2013-1790	CVE-2013-4352	CVE-2014-0117	CVE-2014-0118	CVE-2014-0226	CVE-2014-0231
CVE-2015-1798	CVE-2015-1799	CVE-2015-3405	CVE-2015-5600		

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.



Applicability

Delivery of the FFPS Security Patch Cluster using media (DVD/USB) install must be performed by Xerox Service, and most likely the Analyst that supports a customer account. It is not intended for the customer to perform the Security Patch Cluster install. These updates are also delivered electronically over the network from the Xerox Edge host and Download Server, and that form of delivery can be used by the customer to install Security patch updates.

The Xerox Customer Service Engineer (CSE)/Analyst is provided a tool (accessible from CFO Web site) that enables the analyst to confirm the currently installed FFPS software release, Security Patch Cluster, and Java Software version. When this Security update has been installed on the FFPS system, example output from this script for the FFPS v8 software release is as following:

FFPS Release Version: 8.0_SP-2 (82.E2.34)
FFPS Patch Cluster: October 2015
Java Version: Java 6 Update 105

The October 2015 Security Patch Cluster is available for the FFPS Software Releases below:

FFPS v7

These FFPS v7 Security updates are intended for Xerox printer products running the FFPS 73.F1.31C software releases. The October 2015 Security Patch Cluster has not been tested with the FFPS 73.E1.34, 73.D4.31B, 73.D4.31, 73.D2.33, 73.C5.11, 73.C3.51, 73.C0.41, 73.B3.61 and, 73.B0.73 software releases, but there should not be any problems on these releases.

FFPS v8

These FFPS v8 Security updates are intended for Xerox printer products running the FFPS 82.E2.34 (for EPC, 770 / 700i DCP & XC 550/560 and 81.E2.24 (for iGen4) software releases. It is also supported on the FFPS 82.D4.24 / 82.D1.44/ 82.C5.24 / 82.C3.31 SPAR software releases (for EPC products). The October 2015 Security Patch Cluster has not been tested with the FFPS 82.D4.24, 82.D1.44, 82.C5.24, 82.C3.31 and 82.C1.41 software releases, but there should not be any problems on these releases.

FFPS v9

These FFPS v9 Security updates are intended for Xerox printer products running the FFPS 93.F0.94F for iGen Products (iGen4, iGen150 & XC 8250) and 93.F0.14B for XC J75, XC C75, XC 560/570, XV 2100 & D95/110/125 printers. The October 2015 Security Patch Cluster has not been tested with the FFPS 93.E2.22A, 94.E4.45G, 93.E1.24M1, 93.E1.14A, 93.D3.71B, 93.D3.43, 93.D1.42E, 93.C4.93, 90.E2.51, 90.D0.46, 90.C3.64, 90.C0.20 and 90.B4.22A (for D95/110/125 printers) software releases, but there should not be any problems on these releases.

Patch Install

Xerox strives to deliver these critical Security patch updates in a timely manner. The customer process to obtain FFPS 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 FFPS Security Patch Cluster using a script utility that will support installing the patch cluster from the FFPS hard disk, DVD, or USB media.

Once the Security patch updates are ready for customer delivery they are made available on the CFO Web site. The Xerox CSE/Analyst can download and prepare for the install by writing the Security patch update into a known directory on the FFPS system, or on DVD/USB media. The FFPS Security Patch Cluster is delivered as an ISO image and ZIP archive file to provide the Xerox CSE/Analyst options to choose an install method. Once the patch cluster has been prepared on media an install script can be run to perform the install. The install script accepts an argument that identifies the media that contains a copy of the FFPS 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. The Security patch update could be corrupted when writing to media by particular DVD burn applications writing on some DVD media types. It is very important that the Security patch archive written onto the DVD install media be verified with the original archive file that was written to DVD. The Solaris checksum of the Security Patch Cluster ZIP and ISO are provided here in this bulletin as reference to check against the actual checksum.

Supplement October security cluster contains additional fix and this is not full October Security cluster. October Security cluster 2015 should be installed before installation of supplement patch. Supplement patch is script and it does not contain an ISO file.



The Security patch cluster is delivered as a ZIP and an ISO file. The file size and check sum of these files on Windows and Solaris are as follows:

FFPS v7

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
October2015AndJava6U105Patches_v7.zip	1,881,285	1,926,435,048	35407 3762569
October2015AndJava6U105Patches_v7.iso	1,881,636	1,926,795,264	63089 3763272

The **October2015AndJava6U105Patches_v7.zip** listed on the DVD media can be verified by comparing it to the original archive file size and checksum. Copy this archive to a location on the FFPS system and type '**sum October2015AndJava6U105Patches_v7.zip**' from a terminal window. The checksum value should be '**35407 3762569**', and this validates the correct October 2015 Security Patch Cluster is written on the DVD.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
October2015AndJava6U105Patches_v8.zip	1,852,987	1,897,458,283	41087 3705974
October2015AndJava6U105Patches_v8.iso	1,853,338	1,897,818,112	2636 3706676

The **October2015AndJava6U105Patches_v8.zip** listed on the DVD media can be verified by comparing it to the original archive file size and checksum. Copy this archive to a location on the FFPS system and type '**sum October2015AndJava6U105Patches_v8.zip**' from a terminal window. The checksum value should be '**41087 3705974**', and this validates the correct October 2015 Security Patch Cluster is written on the DVD.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
October2015AndJava6U105Patches_v9.zip	1,919,912	1,965,988,942	37552 3839823
October2015AndJava6U105Patches_v9.iso	1,920,262	1,966,348,288	64845 3840524

The **October2015AndJava6U105Patches_v9.zip** listed on the DVD media can be verified by comparing it to the original archive file size and checksum. Copy this archive to a location on the FFPS system and type '**sum October2015AndJava6U105Patches_v9.zip**' from a terminal window. The checksum value should be '**37552 3839823**', and this validates the correct October 2015 Security Patch Cluster is written on the DVD.



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.