Xerox Security Bulletin XRX14-002

FreeFlow Print Server v7, v8 and v9

January 2014 Security Patch Cluster (includes Java 6 Update 71 Software)
v1.0
02/18/2014

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 no longer provides 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. **Jan 2014 Security Patch Cluster**
   - ✓ This supersedes the October 2013 Security Patch Cluster
2. **Java 6 Update 71 Software**
   - ✓ This supersedes Java 6 Update 65 Software

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

CVE-2014-0410	CVE-2014-0415	CVE-2013-5907	CVE-2014-0428	CVE-2014-0422	CVE-2013-5889
CVE-2014-0417	CVE-2014-0387	CVE-2014-0424	CVE-2014-0373	CVE-2013-5878	CVE-2014-0403
CVE-2014-0375	CVE-2014-0423	CVE-2013-5905	CVE-2013-5906	CVE-2013-5902	CVE-2014-0418
CVE-2013-5887	CVE-2013-5899	CVE-2013-5896	CVE-2013-5884	CVE-2014-0416	CVE-2014-0376
CVE-2014-0368	CVE-2013-5910	CVE-2013-5888	CVE-2013-5898	CVE-2014-0411	CVE-2013-5821
CVE-2013-5872	CVE-2014-0390	CVE-2013-4475	CVE-2012-6139	CVE-2011-1202	CVE-2012-2825
CVE-2012-2870	CVE-2012-2871	CVE-2012-2893	CVE-2011-3970	CVE-2007-6750	CVE-2013-4124

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

FFPS v7

These FFPS v7 Security updates are intended for Xerox printer products running the FFPS 73.D2.33 and 73.C5.11 software releases. The January 2014 Security Patch Cluster has not been tested with the FFPS 73.C3.51, 73.C0.41, 73.B3.6 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.D1.44 (for EPC, 770 / 700i DCP, XC 550/560 and XC 800/1000 and 81.D0.73 (for iGen4) software releases.. It is also supported on the FFPS 82.C5.24 / 82.C3.31 SPAR software releases (for EPC, XC 550/560 and XC 800/1000). The January 2014 Security Patch Cluster has not been tested with the FFPS 82.C5.24 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.C4.93 (for iGen150), FFPS 91.C4.71 (for XC 800/1000 printers) and FFPS 90.D3.06 (for D95/110/125 printers) SPAR software releases. The Jan 2014 Security Patch Cluster has not been tested with the FFPS 91.C1.64B (for XC 800/1000 printers), 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.

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.D1.44)
FFPS Patch Cluster: January 2014
Java Version: Java 6 Update 71

Patch Install

The install of these Security patches must be performed by a Xerox CSE or Analyst. The customer process to obtain this Security update is to call the Xerox support number to request the service. Xerox strives to deliver these critical Security patch updates in a timely manner. The method available for delivery is an FTP transfer to the FFPS system or writing the patch cluster to DVD/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 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
Jan2014AndJava6U71Patches_v7.zip	1,668,577	1,708,622,486	4715 3337154
Jan2014AndJava6U71Patches_v7.iso	1,668,928	1,708,982,272	30595 3337856

The **Jan2014AndJava6U71Patches_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 Jan2014AndJava6U71Patches_v7.zip**' from a terminal window. The

checksum value should be '**4715 3337154**', and this validates the correct January 2014 Security Patch Cluster is written on the DVD.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Jan2014AndJava6U71Patches_v8.zip	1,700,346	1,741,154,303	41463 3400692
Jan2014AndJava6U71Patches_v8.iso	1,700,696	1,741,512,704	1859 3401392

The **Jan2014AndJava6U71Patches_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 Jan2014AndJava6U71Patches_v8.zip**' from a terminal window. The checksum value should be '**41463 3400692**', and this validates the correct Jan 2014 Security Patch Cluster is written on the DVD.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Jan2014AndJava6U71Patches_v9.zip	1,621,153	1,660,060,416	16336 3242306
Jan2014AndJava6U71Patches_v9.iso	1,621,504	1,660,420,096	41227 3243008

The **Jan2014AndJava6U71Patches_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 Jan2014AndJava6U71Patches_v9.zip**' from a terminal window. The checksum value should be '**16336 3242306**', and this validates the correct Jan 2014 Security Patch Cluster is written on the DVD.

Disclaimer