Xerox Security Bulletin XRX13-007

FreeFlow Print Server v7, v8 and v9

July 2013 Security Patch Cluster (includes Java 6 Update 51 Software)

v1.0

08/27/2013

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. **July 2013 Security Patch Cluster**
   - ✓ This supersedes the April 2013 Security Patch Cluster
2. **Java 6 Update 51 Software**
   - ✓ This supersedes Java 6 Update 45 Software

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

CVE-2010-5107	CVE-2012-2814	CVE-2013-0169	CVE-2013-2407	CVE-2013-2451	CVE-2013-2465
CVE-2011-0419	CVE-2012-2836	CVE-2013-0213	CVE-2013-2412	CVE-2013-2452	CVE-2013-2466
CVE-2011-0465	CVE-2012-2837	CVE-2013-0214	CVE-2013-2437	CVE-2013-2453	CVE-2013-2467
CVE-2011-3368	CVE-2012-2840	CVE-2013-0338	CVE-2013-2442	CVE-2013-2454	CVE-2013-2468
CVE-2011-3389	CVE-2012-2841	CVE-2013-0398	CVE-2013-2443	CVE-2013-2455	CVE-2013-2469
CVE-2011-4317	CVE-2012-2845	CVE-2013-1667	CVE-2013-2444	CVE-2013-2456	CVE-2013-2470
CVE-2012-0814	CVE-2012-3374	CVE-2013-3745	CVE-2013-2445	CVE-2013-2457	CVE-2013-2471
CVE-2012-0845	CVE-2012-3817	CVE-2013-3757	CVE-2013-2446	CVE-2013-2459	CVE-2013-2472
CVE-2012-0876	CVE-2012-5134	CVE-2013-3799	CVE-2013-2447	CVE-2013-2461	CVE-2013-2473
CVE-2012-1150	CVE-2012-5667	CVE-2013-3813	CVE-2013-2448	CVE-2013-2462	CVE-2013-2474
CVE-2012-2812	CVE-2012-6329	CVE-2013-1500	CVE-2013-2450	CVE-2013-2463	
CVE-2012-2813	CVE-2013-0166	CVE-2013-1571	CVE-2013-2451	CVE-2013-2464	

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 July 2013 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) and FFPS 81.C4.01 (for iGen4). The July 2013 Security Patch Cluster has not been tested with the FFPS 81.B0.34A 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 91.D2..32 (for XC 800/1000, iGen4 and iGen 150 Printers), FFPS 91.C4.71 (for XC 800/1000 printers) and FFPS 90.D0.46 (for D95/110/125 printers) SPAR software releases. The July 2013 Security Patch Cluster has not been tested with the FFPS 91.C4.71 software and 90.B4.22A (for D95/110/125 printers) launch software release, 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-3 (82.D1.44)
FFPS Patch Cluster: July 2013
Java Version: Java 6 Update 51

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
Jul2013AndJava6U51Patches_v7.zip	1,729,673	1,771,184,717	9464 3459346
Jul2013AndJava6U51Patches_v7.iso	1,730,024	1,772,544,576	34754 3460048

The **Jul2013AndJava6U51Patches_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 Jul2013AndJava6U51Patches_v7.zip**' from a terminal window. The checksum value should be '**9464 3450346**', and this validates the correct July 2013 Security Patch Cluster is written on the DVD.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Jul2013AndJava6U51Patches_v8.zip	1,745,371	1,787,258,894	13298 3490741
Jul2013AndJava6U51Patches_v8.iso	1,745,722	1,787,619,328	38068 3491444

The **Jul2013AndJava6U51Patches_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 Jul2013AndJava6U51Patches_v8.zip**' from a terminal window. The checksum value should be '**13298 3490741**', and this validates the correct July 2013 Security Patch Cluster is written on the DVD.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Jul2013AndJava6U51Patches_v9.zip	1,624,296	1,663,278,667	22691 3248592
Jul2013AndJava6U51Patches_v9.iso	1,624,646	1,663,637,504	47464 3249292

The **Jul2013AndJava6U51Patches_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 Jul2013AndJava6U51Patches_v9.zip**' from a terminal window. The checksum value should be '**22691 3248592**', and this validates the correct July 2013 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.