Xerox Security Bulletin XRX14-004

FreeFlow Print Server v7, v8 and v9

April 2014 Security Patch Cluster

v1.0

06/13/2014

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. **April 2014 Security Patch Cluster**
   - ✓ This supersedes the January 2014 Security Patch Cluster
2. **Java 6 Update 75 Software**
   - ✓ This supersedes Java 6 Update 71 Software

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

CVE-2014-2428	CVE-2014-2427	CVE-2014-2423	CVE-2014-2414	CVE-2014-2412	CVE-2014-2402
CVE-2014-0458	CVE-2014-0454	CVE-2014-0452	CVE-2014-0451	CVE-2014-0446	CVE-2014-0424
CVE-2014-0387	CVE-2014-0373	CVE-2013-5878	CVE-2013-5852	CVE-2013-5802	CVE-2013-5775
CVE-2014-0376	CVE-2014-0382	CVE-2014-0429	CVE-2013-1563	CVE-2013-0429	CVE-2013-0423
CVE-2013-0419	CVE-2013-0351	CVE-2012-5084	CVE-2012-5068	CVE-2012-1711	CVE-2007-1859
CVE-2007-6750	CVE-2012-2733	CVE-2012-3544	CVE-2012-3546	CVE-2012-4431	CVE-2012-4534
CVE-2012-5668	CVE-2012-5669	CVE-2012-5670	CVE-2012-5885	CVE-2012-5886	CVE-2012-5887
CVE-2012-6150	CVE-2013-1417	CVE-2013-1418	CVE-2013-2067	CVE-2013-4408	CVE-2013-5211
CVE-2013-6462	CVE-2014-0591				

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, 73.D4.31B and 73.D4.31software releases. The April 2014 Security Patch Cluster has not been tested with the FFPS 73.C5.11, 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.D2.24 (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.D1.44/ 82.C5.24 / 82.C3.31 SPAR software releases (for EPC, XC 550/560 and XC 800/1000). The April 2014 Security Patch Cluster has not been tested with the FFPS 82.D1.44, 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.E0.21C (for iGen3) and FFPS 90.D3.06 (for D95/110/125 printers) SPAR software releases. The April 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-3 (82.D2.44)
FFPS Patch Cluster: April 2014
Java Version: Java 6 Update 75

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
April2014AndJava6U75Patches_v7.zip	1,675,341	1,715,549,168	29029 3350682
April2014AndJava6U75Patches_v7.iso	1,675,692	1,715,908,608	55190 3351384

The **April2014AndJava6U75Patches_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 April2014AndJava6U75Patches_v7.zip'** from a terminal window. The checksum value should be '**29029 3350682'**, and this validates the correct April 2014 Security Patch Cluster is written on the DVD.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
April2014AndJava6U75Patches_v8.zip	1,709,402	1,750,427,465	23072 3418804
April2014AndJava6U75Patches_v8.iso	1,709,752	1,750,786,048	48446 3419504

The **April2014AndJava6U75Patches_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 April2014AndJava6U75Patches_v8.zip**' from a terminal window. The checksum value should be '**23072 3418804'**, and this validates the correct April 2014 Security Patch Cluster is written on the DVD.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
April2014AndJava6U75Patches_v9.zip	1,632,371	1,671,547,384	26625 3264741
April2014AndJava6U75Patches_v9.iso	1,632,722	1,671,907,328	53290 3265444

The **April2014AndJava6U75Patches_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 April2014AndJava6U75Patches_v9.zip**' from a terminal window. The checksum value should be '**26625 3264741'**, and this validates the correct April 2014 Security Patch Cluster is written on the DVD.

Disclaimer