May 23, 2016

Xerox Security Bulletin XRX16-008

FreeFlow Print Server v7, v8 and v9

Media Delivery (DVD/USB) of:

- April 2016 Security Patch Cluster
- Java 6 Update 115 (FFPS v8, v9)
- Java 7 Update 101 (FFPS v7)

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 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 2016 Security Patch Cluster
   - ✓ This supersedes the January 2016 Security Patch Cluster
2. Java 6 Update 115 Software (V9 & V8)
   - ✓ This supersedes Java 6 Update 111 Software
3. Java 7 Update 101 Software (V7)
   - ✓ This supersedes Java 7 Update 95 Software

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

CVE-2004-0548	CVE-2014-8101	CVE-2015-5600	CVE-2015-7871	CVE-2016-0466	CVE-2016-1286
CVE-2012-2814	CVE-2014-8102	CVE-2015-5602	CVE-2015-7973	CVE-2016-0483	CVE-2016-2110
CVE-2014-3566	CVE-2014-8103	CVE-2015-7236	CVE-2015-7974	CVE-2016-0494	CVE-2016-2111
CVE-2014-6271	CVE-2015-0005	CVE-2015-7691	CVE-2015-7975	CVE-2016-0535	CVE-2016-2112
CVE-2014-6277	CVE-2015-0293	CVE-2015-7692	CVE-2015-7976	CVE-2016-0676	CVE-2016-2113
CVE-2014-6278	CVE-2015-3194	CVE-2015-7701	CVE-2015-7977	CVE-2016-0693	CVE-2016-2115
CVE-2014-7169	CVE-2015-3195	CVE-2015-7702	CVE-2015-7978	CVE-2016-0695	CVE-2016-2118
CVE-2014-7186	CVE-2015-3197	CVE-2015-7703	CVE-2015-7979	CVE-2016-0702	CVE-2016-3419
CVE-2014-8091	CVE-2015-3418	CVE-2015-7704	CVE-2015-7981	CVE-2016-0703	CVE-2016-3441
CVE-2014-8092	CVE-2015-4000	CVE-2015-7705	CVE-2015-8126	CVE-2016-0704	CVE-2016-3443
CVE-2014-8093	CVE-2015-5146	CVE-2015-7848	CVE-2015-8138	CVE-2016-0705	CVE-2016-0687
CVE-2014-8094	CVE-2015-5174	CVE-2015-7849	CVE-2015-8139	CVE-2016-0706	CVE-2016-0686
CVE-2014-8095	CVE-2015-5252	CVE-2015-7850	CVE-2015-8140	CVE-2016-0714	CVE-2016-3427
CVE-2014-8096	CVE-2015-5296	CVE-2015-7851	CVE-2015-8158	CVE-2016-0797	CVE-2016-3449
CVE-2014-8097	CVE-2015-5299	CVE-2015-7852	CVE-2015-8472	CVE-2016-0798	CVE-2016-3422
CVE-2014-8098	CVE-2015-5300	CVE-2015-7853	CVE-2015-8704	CVE-2016-0799	CVE-2016-3425
CVE-2014-8099	CVE-2015-5345	CVE-2015-7854	CVE-2016-0402	CVE-2016-0800	CVE-2016-3426
CVE-2014-8100	CVE-2015-5370	CVE-2015-7855	CVE-2016-0448	CVE-2016-1285	

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 FFPS DFE.

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: 9.0_SP-3 (93.F3.12C)
FFPS Patch Cluster: April 2016
Java Version: Java 6 Update 115

The April 2016 Security Patch Cluster is available for the FFPS Software Releases below:

FFPS v7

Xerox printer products running the FFPS 73.F1.31C software release require install of the FFPS v7.3 April 2016 Security Patch Cluster. All previous FFPS v7.3 software releases have not been tested with April 2016 Security Patch Cluster, but there should not be any problems on previous FFPS 7.3 releases.

FFPS v8

Xerox printer products running the FFPS 82.F4.34 software release for EPC, 770 / 700i DCP, and XC 550/560 printers and 81.F5.01 software release for the iGen4 printer require install of the FFPS v8.2 April 2016 Security Patch Cluster. All previous FFPS v8.2 software releases have not been tested with April 2016 Security Patch Cluster, but there should not be any problems on previous FFPS v8.2 releases.

FFPS v9

Xerox printer products running the FFPS 93.F3.12C for iGen printers (iGen4, iGen150, and XC 8250), 93.F3.12C for XC 800i/1000i printers, 93.F3.12C for J75, XC C75, XC 560/570, D95/110/125 printers, and 93.F1.44B for the XV 2100 printer requires install of the FFPS v9.3 April 2016 Security Patch Cluster. All previous FFPS v9.3 software releases have not been tested with April 2016 Security Patch Cluster, but there should not be any problems on previous FFPS 9.3 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 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:

FFPS v7

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
April2016AndJava7U101Patches_v7.zip	1,996,867	2,044,791,070	49824 3993733
April2016AndJava7U101Patches_v7.iso	1,997,218	2,045,151,232	11164 3994436

Verify the April2016AndJava7U101Patches_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 FFPS system and type 'sum April2016AndJava7U101Patches_v7.zip' from a terminal window. The checksum value should be '49824 3993733', and can be used to validate the correct April 2016 Security Patch Cluster on the DVD/USB.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
April2016AndJava6U115Patches_v8.zip	1,954,426	2,001,331,408	15585 3908851
April2016AndJava6U115Patches_v8.iso	1,954,776	2,001,690,624	43607 3909552

Verify the April2016AndJava6U115Patches_v8.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 FFPS system and type 'sum April2016AndJava6U115Patches_v8.zip' from a terminal window. The checksum value should be '15585 3908851', and can be used to validate the correct April 2016 Security Patch Cluster on the DVD/USB.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
April2016AndJava6U115Patches_v9.zip	2,019,549	2,068,017,246	52809 4039097
April2016AndJava6U115Patches_v9.iso	2,019,900	2,068,377,600	13916 4039800

Verify the April2016AndJava6U115Patches_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 FFPS system and type 'sum April2016AndJava6U115Patches_v9.zip' from a terminal window. The checksum value should be '52809 4039097', and can be used to validate the correct April 2016 Security Patch Cluster on the DVD/USB.

Disclaimer