November 21, 2016

Xerox Security Bulletin XRX16-025

FreeFlow Print Server v7, v8 and v9

Media Delivery (DVD/USB) of:

- October 2016 Security Patch Cluster
- Java 6 Update 131 (FFPS v8)
- Java 7 Update 121 (FFPS v7, v9)

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 authorize vendors like Xerox 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 not prepared/delivered by Xerox. Installing non-authorized patches for the FFPS software violates Oracle agreements, can render the system inoperable, and result in downtime and/or a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. October 2016 Security Patch Cluster
   - ✓ This supersedes the July 2016 Security Patch Cluster
2. Java 6 Update 131 Software (v8)
   - ✓ This supersedes Java 6 Update 121 Software
3. Java 7 Update 121 Software (v7, v9)
   - ✓ This supersedes Java 7 Update 111 Software

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

CVE-2012-0876	CVE-2015-1547	CVE-2016-1836	CVE-2016-2518	CVE-2016-4483	CVE-2016-5542
CVE-2012-4564	CVE-2015-5296	CVE-2016-1837	CVE-2016-2519	CVE-2016-4562	CVE-2016-5554
CVE-2013-1619	CVE-2015-5370	CVE-2016-1838	CVE-2016-2775	CVE-2016-4563	CVE-2016-5556
CVE-2013-1960	CVE-2015-7704	CVE-2016-1839	CVE-2016-3189	CVE-2016-4564	CVE-2016-5559
CVE-2013-1961	CVE-2015-8138	CVE-2016-1840	CVE-2016-3627	CVE-2016-4953	CVE-2016-5568
CVE-2013-2116	CVE-2015-8806	CVE-2016-2073	CVE-2016-3705	CVE-2016-4954	CVE-2016-5573
CVE-2013-4231	CVE-2016-0718	CVE-2016-2110	CVE-2016-3714	CVE-2016-4955	CVE-2016-5582
CVE-2013-4232	CVE-2016-1547	CVE-2016-2111	CVE-2016-3715	CVE-2016-4956	CVE-2016-5597
CVE-2013-4243	CVE-2016-1548	CVE-2016-2112	CVE-2016-3716	CVE-2016-4957	CVE-2016-5841
CVE-2013-4244	CVE-2016-1549	CVE-2016-2113	CVE-2016-3717	CVE-2016-4971	CVE-2016-5842
CVE-2014-9330	CVE-2016-1550	CVE-2016-2115	CVE-2016-3718	CVE-2016-5118	CVE-2016-6185
CVE-2014-9655	CVE-2016-1551	CVE-2016-2118	CVE-2016-4447	CVE-2016-5300	CVE-2016-6302
CVE-2015-0005	CVE-2016-1833	CVE-2016-2516	CVE-2016-4448	CVE-2016-5480	CVE-2016-6491
CVE-2015-1283	CVE-2016-1835	CVE-2016-2517	CVE-2016-4449	CVE-2016-5553	

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 Platform.

Applicability

The customer can schedule a Xerox Service or Analyst representative to deliver and install the FFPS Security Patch Cluster using media (DVD/USB). A customer can only perform the install procedures with approval of the Xerox CSE/Analyst. Xerox does offer an electronic delivery and "easy to use" install of Security Patch Clusters, which is more suited for a customer to manage the quarterly patches on their own.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool (accessible from CFO Web site) that enables identification of the currently installed FFPS software release, Security Patch Cluster, and Java Software version. Run this tool after the Security Patch Cluster install to validate a successful install. Example output from this script for the FFPS v9 software release is as following:

FFPS Release Version:	9.0_SP-3 (93.G3.66B)
FFPS Patch Cluster:	October 2016
Java Version:	Java 7 Update 121

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

FFPS v7

Xerox printer products running the FFPS 73.G2.55 software release require install of the FFPS v7.3 October 2016 Security Patch Cluster. All previous FFPS v7.3 software releases have not been tested with October 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.G3.03 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 October 2016 Security Patch Cluster. All previous FFPS v8.2 software releases have not been tested with October 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.G3.66B for iGen printers (iGen4, iGen150, and XC 8250), XC 800i/1000i printers, J75, XC C75, XC 560/570, D95/110/125 printers, and XV 2100 printer requires install of the FFPS v9.3 October 2016 Security Patch Cluster. All previous FFPS v9.3 software releases have not been tested with October 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.

The Security Patch Cluster deliverables are available on the CFO Web site once they are ready for customer delivery. 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. Delivery of the Security Patch Cluster includes an ISO and ZIP archive file for convenience. Once the patch cluster has been prepared on media, run the provided install script 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. Writing to media using some DVD write applications and media types could result in

a corrupted Security Patch Cluster. 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
Oct2016AndJava7U121Patches_v7.zip	2,123,460	2,174,422,580	32432 4246920
Oct2016AndJava7U121Patches_v7.iso	2,123,810	2,174,781,440	59661 4247620

Verify the **Oct2016AndJava7U121Patches_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 Oct2016AndJava7U121Patches_v7.zip**' from a terminal window. The checksum value should be '**32432 4246920**', and can be used to validate the correct October 2016 Security Patch Cluster on the DVD/USB.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Oct2016AndJava6U131Patches_v8.zip	2,071,918	2,121,643,881	45018 4143836
Oct2016AndJava6U131Patches_v8.iso	2,072,268	2,122,002,432	7253 4144536

Verify the **Oct2016AndJava6U131Patches_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 Oct2016AndJava6U131Patches_v8.zip**' from a terminal window. The checksum value should be '**45018 4143836**', and can be used to validate the correct October 2016 Security Patch Cluster on the DVD/USB.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Oct2016AndJava7U121Patches_v9.zip	2,307,620	2,363,002,797	50330 4615240
Oct2016AndJava7U121Patches_v9.iso	2,307,970	2,363,361,280	12675 4615940

Verify the **Oct2016AndJava7U121Patches_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 Oct2016AndJava7U121Patches_v9.zip**' from a terminal window. The checksum value should be '**50330 4615240**', and can be used to validate the correct October 2016 Security Patch Cluster on the DVD/USB.

Disclaimer