August 9, 2016

Xerox Security Bulletin XRX16-003

FreeFlow Print Server v7, v8 and v9

Media Delivery (DVD/USB) of:

- July 2016 Security Patch Cluster
- Java 6 Update 121 (FFPS v8, v9)
- Java 7 Update 111 (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 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 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. July 2016 Security Patch Cluster
   - ✓ This supersedes the April 2016 Security Patch Cluster
2. Java 6 Update 121 Software (V9 & V8)
   - ✓ This supersedes Java 6 Update 115 Software
3. Java 7 Update 111 Software (V7)
   - ✓ This supersedes Java 7 Update 101 Software

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

CVE-2014-3158
CVE-2015-5370
CVE-2015-7704
CVE-2015-8138
CVE-2015-8629
CVE-2015-8853
CVE-2016-1547
CVE-2016-1548
CVE-2016-1549
CVE-2016-1550
CVE-2016-1551
CVE-2016-2105
CVE-2016-2106
CVE-2016-2107
CVE-2016-2108
CVE-2016-2109
CVE-2016-2110
CVE-2016-2111
CVE-2016-2112
CVE-2016-2115
CVE-2016-2118
CVE-2016-2176
CVE-2016-2177
CVE-2016-2178
CVE-2016-2516
CVE-2016-2517
CVE-2016-2518
CVE-2016-2519
CVE-2016-3115
CVE-2016-3453
CVE-2016-3458
CVE-2016-3485
CVE-2016-3498
CVE-2016-3500
CVE-2016-3503
CVE-2016-3508
CVE-2016-3511
CVE-2016-3550
CVE-2016-3587
CVE-2016-3606
CVE-2016-4953
CVE-2016-4954
CVE-2016-4955
CVE-2016-4956
CVE-2016-4957

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

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.G0.85A)
FFPS Patch Cluster:       July 2016
Java Version:             Java 6 Update 121
```

The July 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 July 2016 Security Patch Cluster. All previous FFPS v7.3 software releases have not been tested with July 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 July 2016 Security Patch Cluster. All previous FFPS v8.2 software releases have not been tested with July 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.G0.85A 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 July 2016 Security Patch Cluster. All previous FFPS v9.3 software releases have not been tested with July 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
July2016AndJava7U111Patches_v7.zip	2,158,532	2,210,336,555	33811 4317064
July2016AndJava7U111Patches_v7.iso	2,158,882	2,210,695,168	60688 4317764

Verify the **July2016AndJava7U111Patches_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 July2016AndJava7U111Patches_v7.zip'** from a terminal window. The checksum value should be **'33811 4317064'**, and can be used to validate the correct July 2016 Security Patch Cluster on the DVD/USB.

FFPS v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
July2016AndJava6U121Patches_v8.zip	2,133,304	2,184,502,702	55654 4266607
July2016AndJava6U121Patches_v8.iso	2,133,654	2,184,861,696	16839 4267308

Verify the **July2016AndJava6U121Patches_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 July2016AndJava6U121Patches_v8.zip**' from a terminal window. The checksum value should be '**55654 4266607'**, and can be used to validate the correct July 2016 Security Patch Cluster on the DVD/USB.

FFPS v9

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
July2016AndJava6U121Patches_v9.zip	2,327,400	2,383,257,360	21447 4654800
July2016AndJava6U121Patches_v9.iso	2,327,750	2,383,616,000	48115 4655500

Verify the **July2016AndJava6U121Patches_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 July2016AndJava6U121Patches_v9.zip**' from a terminal window. The checksum value should be '**21447 4654800'**, and can be used to validate the correct July 2016 Security Patch Cluster on the DVD/USB.

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.