Xerox Security Bulletin XRX20-002

Xerox® FreeFlow® Print Server v8

For: Solaris® 10 Operating System
Install Method: DVD/USB Media

Deliverable: October 2019 Security Patch Cluster
Includes: Java 7 Update 211
Bulletin Date: January 22, 2020

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT Security vulnerabilities and reliability improvements for the Solaris Operating System. Oracle® does provide patches to the public but authorize vendors like Xerox® to deliver if there is an active FreeFlow® Print Server Support Contracts (FSMA). Customers that have an Oracle® Support Contract for their non-FreeFlow® Print Server Solaris Servers should only install patches prepared/delivered by Xerox®. Installing non-authorized patches for the FreeFlow® Print Server software violates Oracle® agreements, and can render the platform inoperable, and result in downtime and/or a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **October 2019 Security Patch Cluster**
   - Supersedes the July 2019 Security Patch Cluster
2. **Java 7 Update 241 Software**
   - Supersedes Java 7 Update 211 Software

See US-CERT Common Vulnerability Exposures (CVE's) mitigated by the October 2019 Security Patch Cluster below:

October 2019 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2017-6508	CVE-2017-15275	CVE-2018-1139	CVE-2018-16852	CVE-2018-10919	CVE-2019-3880
CVE-2017-13089	CVE-2018-0494	CVE-2018-1140	CVE-2018-16853	CVE-2018-20483	CVE-2019-5953
CVE-2017-13090	CVE-2018-1050	CVE-2018-16841	CVE-2018-10858	CVE-2019-2765	CVE-2019-6471
CVE-2017-14746	CVE-2018-1057	CVE-2018-16851	CVE-2018-10918	CVE-2019-3870	

See the US-CERT Common Vulnerability Exposures (CVE's) mitigated by the Java 7 Update 241 Software table below:

Java 7 Update 241 Software Remediated US-CERT CVE's				
CVE-2019-2894	CVE-2019-2949	CVE-2019-2958	CVE-2019-2981	CVE-2019-2989
CVE-2019-2933	CVE-2019-2962	CVE-2019-2973	CVE-2019-2983	CVE-2019-2992
CVE-2019-2945	CVE-2019-2964	CVE-2019-2978	CVE-2019-2988	CVE-2019-2999

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 Xerox® FreeFlow® Print Server Platform.

2.0 Applicability

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

This Security patch deliverable has been tested on the FreeFlow® Print Server 82.I2.15 software releases. We have not tested the October 2019 Security Patch Cluster on all earlier FreeFlow® Print Server 8.2 releases, but there should not be any problems on these releases. It is always good practice to create a System Backup before installing the Security patches.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool (accessible from a secure FTP site) that enables identification of the currently installed FreeFlow® Print Server 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 FreeFlow® Print Server v8 software release is as following:

Solaris OS Version	10 Update 11
FFPS Release Version	8.0-2_SP-2_82.I2.15
FFPS Patch Cluster	October 2019
Java Version	Java 7 Update 241

The October 2019 Security Patch Cluster is available for the FreeFlow® Print Server v8 release running on the Xerox® printer products below:

1. Xerox® iGen®4 Press
2. Xerox® Color 800/1000 Press
3. Xerox® Color 560/570 Printer
4. Xerox ® 700/700i Digital Color Press
5. Xerox ® 770 Digital Color Press

NOTICE: The October 2019 Security Patch Cluster includes patches to mitigate the Meltdown and Spectre vulnerabilities. These vulnerabilities are not mitigated by the Solaris 10 OS patches alone. It is required to install a BIOS firmware update specific to the Xerox printer product and Digital Front End (DFE) platform (E.g., Dell model). Failure to install the Dell BIOS firmware will leave the FreeFlow® Print Server and Xerox printer product susceptible to Meltdown and Spectre beaches to obtain sensitive information. Dell does not deliver BIOS firmware to mitigate Meltdown and Spectre for PC platforms considered EOL (End of Life).

3.0 Patch Install

Xerox® strives to deliver these critical Security patch updates in a timely manner. The customer process to obtain 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 Patch Cluster using a script utility that will support installing the patch cluster from the FreeFlow® Print Server hard disk, DVD, or USB media.

The Security Patch Cluster deliverables are available on a secure FTP 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 FreeFlow® Print Server platform, 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 FreeFlow® Print Server Security Patch Cluster. (e.g., # installSecPatches.sh [diskl dvdl 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:

FreeFlow® Print Server v8

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
Oct2019AndJava7U241Patches_v8.zip	2,325,397	2,381,205,692	7342 4650793
Oct2019AndJava7U241Patches_v8.iso	2,325,748	2,381,565,952	34084 4651496

Verify the **Oct2019AndJava7U241Patches_v8.zip** file contained on the DVD/USB media or hard drive by comparing it to the original archive file size and checksum in the above table. Change directory to the file location (DVD, USB, or hard disk) and type "**sum Oct2019AndJava7U241Patches_v8.zip"** from a terminal window. The checksum value should be "**7342 4650793**", and can be used to validate the correct October 2019 Security Patch Cluster on the DVD/USB or the hard drive.

4.0 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.