Xerox Security Bulletin XRX20-008

Xerox® FreeFlow® Print Server v7

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

Deliverable: April 2020 Security Patch Cluster
Includes: Java 7 Update 261
Bulletin Date: May 19, 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. **April 2020 Security Patch Cluster**
   - Supersedes the January 2020 Security Patch Cluster
2. **Java 7 Update 261 Software**
   - Supersedes Java 7 Update 251 Software

Notice: The April 2020 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 breach of sensitive information using Meltdown and Spectre vulnerabilities. Dell does not deliver BIOS firmware to mitigate Meltdown and Spectre for PC platforms considered EOL (End of Life).

See US-CERT Common Vulnerability Exposures (CVE) the April 2020 Security Patch Cluster remediate in table below:

April 2020 Security Patch Cluster Remediated US-CERT CVE's			
CVE-2018-5743	CVE-2019-8936	CVE-2020-2696	CVE-2020-2851
CVE-2019-6477	CVE-2020-2647	CVE-2020-2771	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 261 software below:

Java 7 Update 261 Software Remediated US-CERT CVE's			
CVE-2020-2756	CVE-2020-2756	CVE-2020-2756	CVE-2020-2756
CVE-2020-2757	CVE-2020-2757	CVE-2020-2757	CVE-2020-2757

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.

The FreeFlow® Print Server **73.I4.44A** (**Nuvera** and **DP/DT HLC** products), **73.G2.55** (**EPC** and **Fuhjin** products), and **73.H3.72** (**DP 1xx/DT 61xx Monochrome** products) software releases have been tested for the Xerox printer products listed on the title page of this document. We have not tested the April 2020 Security Patch Cluster on all earlier FreeFlow® Print Server 7.3 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 v7 software release is as following:

Solaris OS Version	10 Update 11
FFPS Release Version	7.0_SP-3_73.I4.44A
FFPS Patch Cluster	April 2020
Java Version	Java 7 Update 261
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

The April 2020 Security Patch Cluster is available for the FreeFlow® Print Server v7 release running on the Xerox® printer products below:

1. Xerox Nuvera® 100/120 Digital Coper/Printer
2. Xerox Nuvera® 100/120/144 Digital Production System
3. Xerox Nuvera® 100/120/144/157 EA Digital Production System
4. Xerox Nuvera® 200/288/314 EA Perfecting Production System
5. Xerox Nuvera® 100/120/144 MX Digital Production System
6. Xerox Nuvera® 200/288 MX Perfecting Production System
7. Xerox® DocuPrint® 100/115/135/155/180 MX Enterprise Printing System
8. Xerox® DocuTech® 6128/6155/6180 Production Publisher
9. Xerox® DocuTech® 128/155/180 Highlight Color Production Publisher
10. Xerox® DocuColor® 8080 Presses
11. Xerox® Digital Printer 4112/4127 Enterprise Printing System
12. Xerox® Digital 4590/4595 Copier/Printer

NOTICE: The April 2020 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 [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:

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Apr2020AndJava7U261Patches_v7.zip	2,304,052	2,359,348,421	13577 4608103
Apr2020AndJava7U261Patches_v7.iso	2,304,402	2,359,707,648	40200 4608804

Verify the **Apr2020AndJava7U261Patches_v7.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 **Apr2020AndJava7U261Patches_v7.zip**" from a terminal window. The checksum value should be "**13577 4608103**" and can be used to validate the correct April 2020 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.