

Xerox Security Bulletin XRX20-007

Xerox® FreeFlow® Print Server v9

For: Solaris® 10 Operating System

Install Method: DVD/USB Media

Deliverable: January 2020 Security Patch Cluster

Includes: Java 7 Update 251

Bulletin Date: February 12, 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. **January 2020 Security Patch Cluster**
 - Supersedes the October 2019 Security Patch Cluster
2. **Java 7 Update 251 Software**
 - Supersedes Java 7 Update 241 Software

Notice: The January 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 January 2020 Security Patch Cluster remediate in table below:

January 2020 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2015-1196	CVE-2016-10713	CVE-2018-6951	CVE-2019-5010	CVE-2019-10160	CVE-2020-2656
CVE-2015-1396	CVE-2018-0492	CVE-2018-6952	CVE-2019-9636	CVE-2019-13636	CVE-2020-2647
CVE-2015-1802	CVE-2018-1060	CVE-2018-14647	CVE-2019-9740	CVE-2019-13638	CVE-2020-2696
CVE-2015-1803	CVE-2018-1061	CVE-2018-1000030	CVE-2019-9947	CVE-2019-15903	
CVE-2015-1804	CVE-2018-2901	CVE-2018-1000156	CVE-2019-9948	CVE-2019-16935	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 251 software remediate in table below:

Java 7 Update 251 Software Remediated US-CERT CVE's				
CVE-2020-2593	CVE-2020-2590	CVE-2020-2601	CVE-2020-2604	CVE-2020-2654

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 93.J0.90 software release. We have not tested the January 2020 Security Patch Cluster on all earlier FreeFlow® Print Server 9.3 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	9.0_SP-3_(93.J0.90.86)
FFPS Patch Cluster	January 2020
Java Version	Java 7 Update 251
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

The January 2020 Security Patch Cluster is available for the FreeFlow® Print Server v9 release running on the Xerox® printer products below:

1. Xerox® iGen®4
2. Xerox® iGen®4 Diamond Edition®
3. Xerox® iGen®150 Press
4. Xerox® Versant® 80/180/2100 Presses
5. Xerox® Color 800/100 Press
6. Xerox® Color 800i/1000i Press
7. Xerox® Color Press J75/C75 Press
8. Xerox® Color Press 560/570 Production Printer
9. Xerox® Brenva® HD Production Inkjet Press
10. Xerox® Impika® Compact Inkjet Press
11. Xerox® CiPress® 325/500 Production Inkjet System
12. Xerox® D95/110/125/136 Copier/Printer
13. Xerox® Color 8250 Production Press

NOTICE: The January 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 [diskl 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-K-bytes)	Solaris Size (bytes),	Solaris Checksum
Jan2020AndJava7U251Patches_v9.zip	2,243,197	2,297,033,629	29471 4486394
Jan2020AndJava7U251Patches_v9.iso	2,243,548	2,297,393,152	56002 4487096

Verify the **Jan2020AndJava7U251Patches_v9.zip** file by comparing it to the original archive file size and checksum in the above table. Change directory to the file location (DVD media, USB, or hard disk) and type “**sum Jan2020AndJava7U251Patches_v9.zip**” from a terminal window. The checksum value should be “**29471 4486394**”, and can be used to validate the correct January 2020 Security Patch Cluster on the DVD/USB.

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.