

Xerox Security Bulletin XRX23-004

Xerox® FreeFlow® Print Server v7

For: Solaris® 10 Operating System

Install Method: DVD/USB Media

Deliverable: January 2023 Security Patch Cluster

Includes: N/A

Bulletin Date: March 20, 2023

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 2023 Security Patch Cluster

- Supersedes the October 2022 Security Patch Cluster
- There are no CVE's associated with this delivery. It includes patch Id 148460-25 which resolves a time zone issue.
- January 2022 Security Patch Cluster is a prerequisite to ensure the Java 7 Update 331 Software is installed.

2. No Java Software Update

- Use the 'getSecPatchInfo.sh' script to check if the Java 7 Update 311 Software is already installed.
- If the Java 7 Update 311 software is not installed, install the January 2022 Security Patch Cluster first. It includes the Java 7 Update 311 software.

3. Apache Version 2.4.55

Notice: The January 2023 Security Patch Cluster includes patches to mitigate the Meltdown Variant #3 (CVE-2017-5754), and Spectre Variant #1 (CVE-2017-5753) vulnerabilities. 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) for mitigation of Spectre Variant #2 (CVE-2017-5715).

See US-CERT Common Vulnerability Exposures (CVE) for Apache Version 2.4.55 to remediate CVE's in table below:

Apache Version 2.4.55 Remediated US-CERT CVE's

CVE-2006-20001	CVE-2022-36760	CVE-2022-37436		
----------------	----------------	----------------	--	--

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.K5.22 software release has been tested for the Xerox Nuvera printer products listed in this document. We have not tested the January 2023 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_CP.73.k5.22
FFPS Patch Cluster	January 2023
Java Version	Java 7 Update 331
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

The January 2023 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

NOTICE: The January 2023 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
Jan2023SecurityPatches_v7.zip	2,070,765	2,120,462,530	41431 4141529
Jan2023SecurityPatches_v7.iso	2,071,116	2,120,822,784	1860 4142232

Verify the **Jan2023SecurityPatches_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 **Jan2023SecurityPatches_v7.zip**” from a terminal window. The checksum value should be “**41431 4141529**” and can be used to validate the correct January 2023 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.