Xerox Security Bulletin XRX23-001

Xerox® FreeFlow® Print Server v7

For: Solaris® 11.4 Operating System
Install Method: DVD/USB Media
Supports: Xerox Nuvera® PSIP 14.4 Printer Products

Deliverable: January 2023 Security Patch Cluster
Includes: OpenJDK 8 Update 362-b09
Bulletin Date: February 22, 2023

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements for the Solaris® Operating System platform. Oracle® does not provide these patches to the public but authorize vendors like Xerox® to deliver them to customers with an active FreeFlow® Print Server Support Contracts (FSMA). Customers who may have an Oracle® Support Contract for their non-FreeFlow® Print Server / Solaris® Servers should not install patches not prepared/delivered by Xerox®. Installing non-authorized patches for the FreeFlow® Print Server software violates Oracle® agreements, 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 October 2022 Security Patch Cluster
   - This Patch Cluster is only intended for FFPS 73.M1.90 / RV 14.4.28 software. You will first have to perform a software scrape to this release before installing the January 2023 Security Patch Cluster.
2. **OpenJDK 8 Update 362-b09 Software**
   - Supersedes the OpenJDK 8 Update 342-b07 Software.
3. **Apache 2.4.55 Software**
4. **Firefox 102.62.0.esr Software**
   - Supersedes Firefox 91.13.0.esr Software

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v102.62.0.esr software below:

Firefox v102.62.0.esr Software Remediated US-CERT CVE's					
CVE-2022-40674	CVE-2022-40962	CVE-2022-45404	CVE-2022-45410	CVE-2022-45417	CVE-2022-46874
CVE-2022-40956	CVE-2022-42927	CVE-2022-45405	CVE-2022-45411	CVE-2022-45418	CVE-2022-46875
CVE-2022-40957	CVE-2022-42928	CVE-2022-45406	CVE-2022-45412	CVE-2022-45419	CVE-2022-46878
CVE-2022-40958	CVE-2022-42929	CVE-2022-45407	CVE-2022-45413	CVE-2022-45420	CVE-2022-46880
CVE-2022-40959	CVE-2022-42932	CVE-2022-45408	CVE-2022-45415	CVE-2022-45421	CVE-2022-46881
CVE-2022-40960	CVE-2022-45403	CVE-2022-45409	CVE-2022-45416	CVE-2022-46872	CVE-2022-46882

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 362-b09 software below:

OpenJDK 8 Update 362-b09 Software Remediated US-CERT CVE's			
CVE-2023-21830	CVE-2023-21835	CVE-2023-21843	

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache 2.4.55 software below:

Apache 2.4.55 Software Remediated US-CERT CVE's			
CVE-2006-20001	CVE-2022-36760	CVE-2022-37436	

See the US-CERT Common Vulnerability Exposures (CVE) the January 2023 Security Patch Cluster remediate in table below:

January 2023 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2015-20107	CVE-2022-1923	CVE-2022-26981	CVE-2022-3276	CVE-2022-40959	CVE-2022-45411
CVE-2018-7160	CVE-2022-1924	CVE-2022-27404	CVE-2022-34526	CVE-2022-40960	CVE-2022-45412
CVE-2019-6111	CVE-2022-1925	CVE-2022-27405	CVE-2022-35255	CVE-2022-40962	CVE-2022-45413
CVE-2020-10735	CVE-2022-2056	CVE-2022-27406	CVE-2022-35256	CVE-2022-41323	CVE-2022-45414
CVE-2021-28544	CVE-2022-2057	CVE-2022-2867	CVE-2022-3570	CVE-2022-41556	CVE-2022-45415
CVE-2021-37750	CVE-2022-2058	CVE-2022-2868	CVE-2022-3597	CVE-2022-42252	CVE-2022-45416
CVE-2021-42574	CVE-2022-2122	CVE-2022-2869	CVE-2022-3598	CVE-2022-42927	CVE-2022-45417
CVE-2021-42694	CVE-2022-2125	CVE-2022-29154	CVE-2022-3599	CVE-2022-42928	CVE-2022-45418
CVE-2021-46823	CVE-2022-21619	CVE-2022-29187	CVE-2022-3602	CVE-2022-42929	CVE-2022-45419
CVE-2021-46848	CVE-2022-21624	CVE-2022-29458	CVE-2022-36059	CVE-2022-42932	CVE-2022-45420
CVE-2022-0561	CVE-2022-21626	CVE-2022-3032	CVE-2022-36087	CVE-2022-43548	CVE-2022-45421
CVE-2022-0562	CVE-2022-21628	CVE-2022-3033	CVE-2022-3626	CVE-2022-43680	CVE-2022-46872
CVE-2022-0865	CVE-2022-21658	CVE-2022-3034	CVE-2022-3627	CVE-2022-44638	CVE-2022-46874
CVE-2022-0891	CVE-2022-2175	CVE-2022-3155	CVE-2022-37454	CVE-2022-45061	CVE-2022-46875
CVE-2022-0907	CVE-2022-2183	CVE-2022-31628	CVE-2022-37797	CVE-2022-45063	CVE-2022-46878
CVE-2022-0908	CVE-2022-2206	CVE-2022-31629	CVE-2022-3786	CVE-2022-45403	CVE-2022-46880
CVE-2022-0909	CVE-2022-2207	CVE-2022-31630	CVE-2022-39253	CVE-2022-45404	CVE-2022-46881
CVE-2022-0924	CVE-2022-2208	CVE-2022-3190	CVE-2022-39260	CVE-2022-45405	CVE-2022-46882
CVE-2022-1056	CVE-2022-2210	CVE-2022-3204	CVE-2022-3970	CVE-2022-45406	CVE-2023-21900
CVE-2022-1348	CVE-2022-22844	CVE-2022-32212	CVE-2022-40674	CVE-2022-45407	
CVE-2022-1920	CVE-2022-23901	CVE-2022-32213	CVE-2022-40956	CVE-2022-45408	
CVE-2022-1921	CVE-2022-24070	CVE-2022-32215	CVE-2022-40957	CVE-2022-45409	
CVE-2022-1922	CVE-2022-24765	CVE-2022-32222	CVE-2022-40958	CVE-2022-45410	

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.

2.0 Applicability

The customer can schedule a Xerox Service or Analyst representative to deliver and install the Security Patch Cluster from USB/DVD media or the hard disk on the FreeFlow® Print Server platform. A customer can work with the Xerox CSE/Analyst to install the quarterly Security Patch Clusters if they have the expertise. The Xerox CSE/Analyst would be required to provide the Security Patch Cluster deliverables if they agree to allow their customer install.

The January 2023 Security Patch Cluster is available for the FreeFlow® Print Server 73.M1.90 / RV 14.4.28, and higher software releases on the Solaris® 11.4 OS for the Xerox® printer products below:

1. Nuvera® 100/120/144/157 EA Digital Production System
2. Nuvera® 200/288/314 EA Perfecting Production System
3. Nuvera® 100/120/144 MX Digital Production System
4. Nuvera® 200/288 MX Perfecting Production System

This Security patch deliverable has been tested on the FreeFlow® Print Server 73.M1.90.11 software releases. The January 2023 Security Patch Cluster is the first installed for this new FFPS v7 / Solaris 11.4 configuration.

The January 2023 Security Patch Cluster is too large to be supported by Update Manager. These larger deliverables can be transported to the customer location on DVD/USB media, or a laptop computer hard drive, and installed from a directory location on the FreeFlow® Print Server platform. There are four parts (4 ZIP files) delivered for this Security Patch Cluster. They can be transferred to the FreeFlow® Print Server over the network using SFTP or copied from USB/DVD media to prepare for install.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool that enables identification of the currently installed Solaris® OS version, FreeFlow® Print Server software version, Security Patch Cluster version, OpenJDK Software version. Example output from this script for the FreeFlow® Print Server v7 software is as follows:

Solaris® OS Version:	11.4.50.126.3
FFPS Release Version	7.0_SP-3 (73.M1.90.11.86)
FFPS Patch Cluster	January 2023
OpenJDK Version	OpenJDK 8 Update 342

The above versions are the correct information after installing the January 2023 Security Patch Cluster.

3.0 Patch Install

Xerox® strives to deliver 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 install from USB/DVD media, or from the hard disk on the FreeFlow® Print Server platform.

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 transferring the Security patch update into a known directory on the FreeFlow® Print Server platform on to USB media. 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 | usb]).

Delivery of the January 2023 Security Patch Cluster includes four ZIP files. The ZIP files can be transferred to a well-defined location on the FreeFlow® Print Server hard drive to prepare for install. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install. Alternatively, the January 2023 Security Patch Cluster can be installed from USB media.

Note: The install of this Security Patch Cluster can fail if the archive file containing the software is corrupted from when downloading the deliverables from the SFTP site, copying them to USB media or uploading them to the hard drive on the FreeFlow® Print Server platform over a network connection. The table below (i.e., See Next Page) illustrate file size on Windows®, file size on Solaris® and checksum on Solaris® for the January 2023 Security Patch Cluster files.

January 2023 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jan2023AndOpenJDK8Update362Patches_v7S11_4-Part1.zip	3,715,033	3,804,193,317	58450 7430066
Jan2023AndOpenJDK8Update362Patches_v7S11_4-Part2.zip	5,490,574	5,622,347,229	111 10981147
Jan2023AndOpenJDK8Update362Patches_v7S11_4-Part3.zip	3,321,104	3,400,809,843	3637 6642207
Jan2023AndOpenJDK8Update362Patches_v7S11_4-Part4.zip	4,749,584	4,863,573,584	20450 9499168

Verify integrity of the Security Patch files from the FreeFlow® Print Server hard drive by comparing it to the original archive file size checksum with the actual checksum of these files on the platform. Change directory to the location of the Security Patch Cluster file and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., **sum Jan2023AndOpenJDK8Update362Patches_v7S11_4-Part1.zip**). The output of the '**sum**' command should match the checksum in the above table.

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.