Xerox Security Bulletin XRX22-023

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: October 2022 Security Patch Cluster
Includes: OpenJDK 8 Update 342-b07
Bulletin Date: November 17, 2022

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. **October 2022 Security Patch Cluster**
   - Supersedes July 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 befo//re installing the October 2022 Security Patch Cluster.
2. **OpenJDK 8 Update 342-b07 Software**
   - Supersedes the Java 8 Update 322 Software.
3. **Firefox 91.13.0.esr Software**
   - Supersedes Firefox 91.10.0.esr Software

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v91.13.0.esr software below:

Firefox v91.13.0.esr Software Remediated US-CERT CVE's					
CVE-2022-2200	CVE-2022-31739	CVE-2022-31744	CVE-2022-34478	CVE-2022-36318	CVE-2022-38478
CVE-2022-31736	CVE-2022-31740	CVE-2022-34468	CVE-2022-34479	CVE-2022-36319	
CVE-2022-31737	CVE-2022-31741	CVE-2022-34470	CVE-2022-34481	CVE-2022-38472	
CVE-2022-31738	CVE-2022-31742	CVE-2022-34472	CVE-2022-34484	CVE-2022-38473	

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 342-b07 software below:

OpenJDK 8 Update 342-b07 Software Remediated US-CERT CVE's			
CVE-2022-21619	CVE-2022-21624	CVE-2022-21626	CVE-2022-21628

See US-CERT Common Vulnerability Exposures (CVE) the October 2022 Security Patch Cluster remediate in table below:

October 2022 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2018-1000007	CVE-2022-1629	CVE-2022-21454	CVE-2022-27775	CVE-2022-30556	CVE-2022-34472
CVE-2021-4219	CVE-2022-1674	CVE-2022-21460	CVE-2022-27776	CVE-2022-30595	CVE-2022-34478
CVE-2022-0778	CVE-2022-1733	CVE-2022-21540	CVE-2022-27778	CVE-2022-3080	CVE-2022-34479
CVE-2022-0943	CVE-2022-1735	CVE-2022-21541	CVE-2022-27779	CVE-2022-31625	CVE-2022-34481
CVE-2022-1154	CVE-2022-1769	CVE-2022-21610	CVE-2022-27780	CVE-2022-31626	CVE-2022-34484
CVE-2022-1160	CVE-2022-1771	CVE-2022-2200	CVE-2022-27781	CVE-2022-31627	CVE-2022-34484
CVE-2022-1292	CVE-2022-1785	CVE-2022-2226	CVE-2022-27782	CVE-2022-31744	CVE-2022-36318
CVE-2022-1328	CVE-2022-1796	CVE-2022-22576	CVE-2022-2795	CVE-2022-31813	CVE-2022-36319
CVE-2022-1343	CVE-2022-1851	CVE-2022-2274	CVE-2022-28330	CVE-2022-32212	CVE-2022-36359
CVE-2022-1381	CVE-2022-1886	CVE-2022-2319	CVE-2022-28614	CVE-2022-32213	CVE-2022-37434
CVE-2022-1420	CVE-2022-1898	CVE-2022-2320	CVE-2022-28615	CVE-2022-32214	CVE-2022-38177
CVE-2022-1434	CVE-2022-1927	CVE-2022-24302	CVE-2022-28739	CVE-2022-32215	CVE-2022-38178
CVE-2022-1473	CVE-2022-1942	CVE-2022-24303	CVE-2022-2881	CVE-2022-32222	CVE-2022-38472
CVE-2022-1586	CVE-2022-2068	CVE-2022-24765	CVE-2022-2906	CVE-2022-32223	CVE-2022-38473
CVE-2022-1587	CVE-2022-2097	CVE-2022-2509	CVE-2022-29404	CVE-2022-34169	CVE-2022-38478
CVE-2022-1616	CVE-2022-21417	CVE-2022-26373	CVE-2022-29885	CVE-2022-34265	CVE-2022-39401
CVE-2022-1619	CVE-2022-21427	CVE-2022-26377	CVE-2022-30115	CVE-2022-34305	CVE-2022-39417
CVE-2022-1620	CVE-2022-21444	CVE-2022-26691	CVE-2022-30333	CVE-2022-34468	
CVE-2022-1621	CVE-2022-21451	CVE-2022-27774	CVE-2022-30522	CVE-2022-34470	

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 October 2022 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 October 2022 Security Patch Cluster is the first installed for this new FFPS v7 / Solaris 11.4 configuration.

The October 2022 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	October 2022
OpenJDK Version	OpenJDK 8 Update 342

The above versions are the correct information after installing the October 2022 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 October 2022 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 October 2022 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 October 2022 Security Patch Cluster files.

October 2022 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Oct2022AndOpenJDK8Update342Patches_v7S11_4-Part1.zip	3,588,418	3,674,539,793	59743 7176836
Oct2022AndOpenJDK8Update342Patches_v7S11_4-Part2.zip	3,598,203	3,684,558,951	44025 7196405
Oct2022AndOpenJDK8Update342Patches_v7S11_4-Part3.zip	3,113,693	3,188,420,678	28763 6227385
Oct2022AndOpenJDK8Update342Patches_v7S11_4-Part4.zip	4,180,649	4,280,984,074	23376 8361298

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 Oct2022AndOpenJDK8Update342Patches_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.

xerox™