Xerox Security Bulletin XRX23-017

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 2023 Security Patch Cluster
Includes: Apache 2.4.58 and Firefox 102.12.0.esr Software
Bulletin Date: November 9, 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. **October 2023 Security Patch Cluster**
   - Supersedes July 2023 Security Patch Cluster
   - This Patch Cluster is only intended for FFPS 73.M1.90 / RV 14.4.28 software (or later). You will first have to perform a software scrape to this release (or later) before installing the October 2023 Security Patch Cluster.
2. **OpenJDK 8 Update 392-b07 Software**
   - Supersedes OpenJDK 8 Update 382-b09 Software.
3. **Apache 2.4.58 Software**
   - Superseded Apache 2.4.57 Software
4. **Firefox 102.15.0.esr Software**
   - Supersedes Firefox 102.12.0esr Software

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v102.15.0.esr software below:

Firefox v102.15.0.esr Software Remediated US-CERT CVE's				
CVE-2023-4045	CVE-2023-4049	CVE-2023-4056	CVE-2023-4576	
CVE-2023-4046	CVE-2023-4050	CVE-2023-4573	CVE-2023-4581	CVE-2023-37202
CVE-2023-4047	CVE-2023-4054	CVE-2023-4574	CVE-2023-4584	CVE-2023-37207
CVE-2023-4048	CVE-2023-4055	CVE-2023-4575	CVE-2023-37201	CVE-2023-37208

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 392-b07 software below:

OpenJDK 8 Update 392-b07 Software Remediated US-CERT CVE's			
CVE-2023-22025	CVE-2023-22067	CVE-2023-22081	

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache 2.4.58 software below:

Apache 2.4.58 Software Remediated US-CERT CVE's			
CVE-2023-31122	CVE-2023-43622	CVE-2023-45802	

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

October 2023 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2017-5715	CVE-2023-1175	CVE-2023-28450	CVE-2023-30587	CVE-2023-32636	CVE-2023-4047
CVE-2018-3639	CVE-2023-1393	CVE-2023-2854	CVE-2023-30588	CVE-2023-32643	CVE-2023-40477
CVE-2021-44917	CVE-2023-1906	CVE-2023-2855	CVE-2023-30589	CVE-2023-32665	CVE-2023-4048
CVE-2021-46784	CVE-2023-1981	CVE-2023-2857	CVE-2023-30590	CVE-2023-32681	CVE-2023-4049
CVE-2022-31008	CVE-2023-2004	CVE-2023-2858	CVE-2023-31124	CVE-2023-32762	CVE-2023-4050
CVE-2022-32206	CVE-2023-22043	CVE-2023-2879	CVE-2023-31130	CVE-2023-32763	CVE-2023-4054
CVE-2022-32221	CVE-2023-22128	CVE-2023-28879	CVE-2023-31147	CVE-2023-34241	CVE-2023-4055
CVE-2022-3924	CVE-2023-22129	CVE-2023-2911	CVE-2023-3138	CVE-2023-34969	CVE-2023-4056
CVE-2022-41409	CVE-2023-23914	CVE-2023-29402	CVE-2023-31484	CVE-2023-36053	CVE-2023-41080
CVE-2022-48337	CVE-2023-23915	CVE-2023-29403	CVE-2023-31486	CVE-2023-36191	CVE-2023-41081
CVE-2022-48338	CVE-2023-23916	CVE-2023-29404	CVE-2023-3195	CVE-2023-3666	CVE-2023-4504
CVE-2022-48339	CVE-2023-24329	CVE-2023-29405	CVE-2023-32002	CVE-2023-36664	CVE-2023-4573
CVE-2022-4899	CVE-2023-24805	CVE-2023-29406	CVE-2023-32003	CVE-2023-37201	CVE-2023-4574
CVE-2023-0049	CVE-2023-25193	CVE-2023-29409	CVE-2023-32004	CVE-2023-37202	CVE-2023-4575
CVE-2023-0051	CVE-2023-2650	CVE-2023-29491	CVE-2023-32005	CVE-2023-37207	CVE-2023-4576
CVE-2023-0054	CVE-2023-27985	CVE-2023-29499	CVE-2023-32006	CVE-2023-37208	CVE-2023-4581
CVE-2023-0288	CVE-2023-27986	CVE-2023-30581	CVE-2023-32067	CVE-2023-37211	CVE-2023-4584
CVE-2023-0512	CVE-2023-2828	CVE-2023-30582	CVE-2023-3247	CVE-2023-3823	
CVE-2023-0666	CVE-2023-28319	CVE-2023-30583	CVE-2023-32558	CVE-2023-3824	
CVE-2023-0668	CVE-2023-28320	CVE-2023-30584	CVE-2023-32559	CVE-2023-38403	
CVE-2023-1127	CVE-2023-28321	CVE-2023-30585	CVE-2023-32573	CVE-2023-4045	
CVE-2023-1170	CVE-2023-28322	CVE-2023-30586	CVE-2023-32611	CVE-2023-4046	

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 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 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 October 2023 Security Patch Cluster is the first installed for this new FFPS v7 / Solaris 11.4 configuration.

The October 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:	11.4.62.151.3
FFPS Release Version	7.0_SP-3 (73.M1.90.11.86)
FFPS Patch Cluster	October 2023
Java Version	OpenJDK 8 Update 392
Base Repository	Installed
Firefox Version	102.15.0.esr
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

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

October 2023 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Oct2023AndOpenJDK8Update392Patches_v7S11_4-Part1.zip	3,223,232	3,300,588,774	60673 6446463
Oct2023AndOpenJDK8Update392Patches_v7S11_4-Part2.zip	5,071,901	5,193,625,618	28400 10143801
Oct2023AndOpenJDK8Update392Patches_v7S11_4-Part3.zip	4,027,849	4,124,517,313	61597 8055698
Oct2023AndOpenJDK8Update392Patches_v7S11_4-Part4.zip	4,611,818	4,722,500,805	22613 9223635

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 Oct2023AndOpenJDK8Update392Patches_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.