Xerox Security Bulletin XRX24-005

Xerox® FreeFlow® Print Server v9

For: Solaris® 11.4 Operating System
Supports: Xerox® Color 800/800i/1000/1000i Digital Press, Xerox® Versant® 3100 Press

Deliverable: January 2024 Security Patch Cluster
Includes: Apache 2.4.58 and Firefox 115.5.0.esr Software
Bulletin Date: February 21, 2024

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 2024 Security Patch Cluster**
   - Supersedes October 2023 Security Patch Cluster
2. **No Java Software Update**
   - No Change
   - Install the January 2022 Security Patch Cluster first if not already installed. It includes the Java 7 Update 331 Software.
3. **Apache 2.4.58 Software**
   - No Change
4. **Firefox 115.5.0esr Software**
   - Supersedes Firefox 102.15.0.esr Software.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v115.5.0.esr software below:

Firefox v115.5.0.esr Software Remediated US-CERT CVE's				
CVE-2023-4051	CVE-2023-4582	CVE-2023-5176	CVE-2023-5730	CVE-2023-6209
CVE-2023-4052	CVE-2023-4583	CVE-2023-5721	CVE-2023-5732	CVE-2023-6210
CVE-2023-4053	CVE-2023-4585	CVE-2023-5724	CVE-2023-6204	CVE-2023-6211
CVE-2023-4057	CVE-2023-5168	CVE-2023-5725	CVE-2023-6205	CVE-2023-6212
CVE-2023-4577	CVE-2023-5169	CVE-2023-5726	CVE-2023-6206	CVE-2023-6213
CVE-2023-4578	CVE-2023-5171	CVE-2023-5727	CVE-2023-6207	
CVE-2023-4580	CVE-2023-5174	CVE-2023-5728	CVE-2023-6208	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 331 software below:

Java 7 Update 331 Software Remediated US-CERT CVE's			
CVE-2022-21291	CVE-2022-21349		

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 January 2024 Security Patch Cluster remediate in table below:

January 2024 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2021-33391	CVE-2023-0188	CVE-2023-22112	CVE-2023-38559	CVE-2023-44487	CVE-2023-49083
CVE-2022-23825	CVE-2023-0189	CVE-2023-2610	CVE-2023-38560	CVE-2023-44488	CVE-2023-5115
CVE-2022-34670	CVE-2023-0190	CVE-2023-26551	CVE-2023-3863	CVE-2023-4511	CVE-2023-5168
CVE-2022-34673	CVE-2023-0191	CVE-2023-26552	CVE-2023-38633	CVE-2023-4512	CVE-2023-5169
CVE-2022-34674	CVE-2023-0194	CVE-2023-26553	CVE-2023-39318	CVE-2023-4513	CVE-2023-5171
cve-2022-34676	CVE-2023-0195	CVE-2023-26554	CVE-2023-39319	CVE-2023-45143	CVE-2023-5174
CVE-2022-34677	CVE-2023-0198	CVE-2023-26555	CVE-2023-39320	CVE-2023-4577	CVE-2023-5176
CVE-2022-34678	CVE-2023-0199	CVE-2023-2906	CVE-2023-39321	CVE-2023-4578	CVE-2023-5217
CVE-2022-34679	CVE-2023-22005	CVE-2023-2953	CVE-2023-39322	CVE-2023-4580	CVE-2023-5344
CVE-2022-34680	CVE-2023-22008	CVE-2023-2975	CVE-2023-39323	CVE-2023-45803	CVE-2023-5441
CVE-2022-34682	CVE-2023-22028	CVE-2023-30584	CVE-2023-39325	CVE-2023-4582	CVE-2023-5721
CVE-2022-34684	CVE-2023-22032	CVE-2023-32004	CVE-2023-39331	CVE-2023-4583	CVE-2023-5724
CVE-2022-37032	CVE-2023-22033	CVE-2023-3316	CVE-2023-39332	CVE-2023-4585	CVE-2023-5725
CVE-2022-42254	CVE-2023-22038	CVE-2023-3341	CVE-2023-39333	CVE-2023-46137	CVE-2023-5726
CVE-2022-42255	CVE-2023-22046	CVE-2023-3428	CVE-2023-39978	CVE-2023-46246	CVE-2023-5727
CVE-2022-42256	CVE-2023-22048	CVE-2023-34410	CVE-2023-40217	CVE-2023-4733	CVE-2023-5728
CVE-2022-42257	CVE-2023-22053	CVE-2023-3446	CVE-2023-40359	CVE-2023-4734	CVE-2023-5730
CVE-2022-42258	CVE-2023-22054	CVE-2023-36054	CVE-2023-4051	CVE-2023-4735	CVE-2023-5732
CVE-2022-42259	CVE-2023-22056	CVE-2023-3648	CVE-2023-4052	CVE-2023-4736	CVE-2023-5752
CVE-2022-42263	CVE-2023-22057	CVE-2023-3649	CVE-2023-4053	CVE-2023-4738	CVE-2023-6204
CVE-2022-42264	CVE-2023-22058	CVE-2023-37327	CVE-2023-4057	CVE-2023-4750	CVE-2023-6205
CVE-2022-42265	CVE-2023-22059	CVE-2023-37328	CVE-2023-41105	CVE-2023-4752	CVE-2023-6206
CVE-2022-4899	CVE-2023-22064	CVE-2023-37369	CVE-2023-41164	CVE-2023-4781	CVE-2023-6207
CVE-2023-0180	CVE-2023-22070	CVE-2023-38039	CVE-2023-4156	CVE-2023-48231	CVE-2023-6208
CVE-2023-0181	CVE-2023-22078	CVE-2023-3817	CVE-2023-4236	CVE-2023-4863	CVE-2023-6209
CVE-2023-0183	CVE-2023-22079	CVE-2023-38197	CVE-2023-43115	CVE-2023-4863	CVE-2023-6212
CVE-2023-0184	CVE-2023-22084	CVE-2023-38545	CVE-2023-43665	CVE-2023-48706	CVE-2024-20920
CVE-2023-0185	CVE-2023-22092	CVE-2023-38546	CVE-2023-43804	CVE-2023-4874	CVE-2024-20946
CVE-2023-0187	CVE-2023-22103	CVE-2023-38552	CVE-2023-44271	CVE-2023-4875	

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. The FreeFlow® Print Server application supported on Solaris® 11 is not yet supported for install from the Update Manager UI.

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 January 2024 Security Patch Cluster is available for the FreeFlow® Print Server v9 release on the Solaris® 11.4 OS for the Xerox® printer products below:

1. Xerox® Color 800i/1000i Press
2. Xerox® Color 800/1000 Press
3. Xerox® Versant® 3100 Press

This Security patch deliverable has been tested on the FreeFlow® Print Server 93.M3.14 software releases. We have not tested the January 2024 Security Patch Cluster on all earlier FreeFlow® Print Server 9.3 releases, but there should not be any problems on these releases running on the Solaris 11.4 OS.

The January 2024 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, Java Software version. This tool can be initially run to determine if the prerequisite October 2018 Security Patch Cluster is currently installed. Example output from this script for the FreeFlow® Print Server v9 software is as follows:

Solaris® OS Version:	11.4.65.157.1
FFPS Release Version	9.0_SP-3_(93.M3.14.86)
FFPS Patch Cluster	January 2024
Java Version	Java 7 Update 331

The above versions are the correct information after installing the January 2024 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 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 installation 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 2024 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 installation. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install. Alternatively, the January 2024 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) illustrates file size on Windows®, file size on Solaris® and checksum on Solaris® for the January 2024 Security Patch Cluster files.

January 2024 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jan2024SecurityPatches_v9S11_4-Part1.zip	5,603,694	5,738,181,884	45623 11207387
Jan2024SecurityPatches_v9S11_4-Part2.zip	5,395,368	5,524,856,414	24462 10790736
Jan2024SecurityPatches_v9S11_4-Part3.zip	3,623,076	3,710,029,606	10125 7246152
Jan2024SecurityPatches_v9S11_4-Part4.zip	4,222,150	4,323,481,291	46890 8444300

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 **Jan2024SecurityPatches_v9S11_4-Part2.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