Xerox Security Bulletin XRX23-009

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: April 2023 Security Patch Cluster
Includes: Apache 2.4.57 and Firefox 102.9.0.esr Software
Bulletin Date: June 12, 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. **April 2023 Security Patch Cluster**
   - Supersedes January 2023 Security Patch Cluster
2. **No Java Software Update**
   - Install the January 2022 Security Patch Cluster first if not already installed. It includes the Java 7 Update 331 Software.
3. **Apache 2.4.57 Software**
   - Supersedes the Apache 2.4.55 Software.
4. **Firefox 102.9.0esr Software**
   - Supersedes Firefox 102.62.0esr Software.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v102.9.0esr software below:

Firefox v102.9.0esr Software Remediated US-CERT CVE's					
CVE-2022-46871	CVE-2023-23601	CVE-2023-25729	CVE-2023-25737	CVE-2023-25744	CVE-2023-28163
CVE-2022-46877	CVE-2023-23602	CVE-2023-25730	CVE-2023-25738	CVE-2023-25746	CVE-2023-28164
CVE-2023-0767	CVE-2023-23603	CVE-2023-25732	CVE-2023-25739	CVE-2023-25751	CVE-2023-28176
CVE-2023-23598	CVE-2023-23605	CVE-2023-25734	CVE-2023-25742	CVE-2023-25752	
CVE-2023-23599	CVE-2023-25728	CVE-2023-25735	CVE-2023-25743	CVE-2023-28162	

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 2.4.57 software below:

Apache 2.4.57 Software Remediated US-CERT CVE's			
CVE-2023-25690	CVE-2023-27522		

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

April 2023 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2006-20001	CVE-2022-2874	CVE-2022-3234	CVE-2022-42898	CVE-2023-0568	CVE-2023-23936
CVE-2017-12613	CVE-2022-2879	CVE-2022-3235	CVE-2022-42915	CVE-2023-0616	CVE-2023-23946
CVE-2018-25032	CVE-2022-2880	CVE-2022-3256	CVE-2022-42916	CVE-2023-0662	CVE-2023-23969
CVE-2021-29338	CVE-2022-2889	CVE-2022-3278	CVE-2022-42919	CVE-2023-0767	CVE-2023-24580
CVE-2021-30860	CVE-2022-2923	CVE-2022-3296	CVE-2022-4304	CVE-2023-0795	CVE-2023-24807
CVE-2021-35940	CVE-2022-2928	CVE-2022-3297	CVE-2022-4345	CVE-2023-0796	CVE-2023-24998
CVE-2021-37519	CVE-2022-2929	CVE-2022-3324	CVE-2022-4450	CVE-2023-0797	CVE-2023-25690
CVE-2021-37750	CVE-2022-2946	CVE-2022-3352	CVE-2022-45143	CVE-2023-0798	CVE-2023-25728
CVE-2022-0718	CVE-2022-29526	CVE-2022-3515	CVE-2022-45199	CVE-2023-0799	CVE-2023-25729
CVE-2022-1122	CVE-2022-2980	CVE-2022-35252	CVE-2022-45939	CVE-2023-0800	CVE-2023-25730
CVE-2022-1292	CVE-2022-29804	CVE-2022-35260	CVE-2022-46340	CVE-2023-0801	CVE-2023-25732
CVE-2022-1705	CVE-2022-3016	CVE-2022-36113	CVE-2022-46341	CVE-2023-0802	CVE-2023-25734
CVE-2022-1962	CVE-2022-3037	CVE-2022-36114	CVE-2022-46342	CVE-2023-0803	CVE-2023-25735
CVE-2022-21515	CVE-2022-30580	CVE-2022-36227	CVE-2022-46343	CVE-2023-0804	CVE-2023-25737
CVE-2022-2309	CVE-2022-30629	CVE-2022-36760	CVE-2022-46344	CVE-2023-21830	CVE-2023-25738
CVE-2022-23521	CVE-2022-30630	CVE-2022-3705	CVE-2022-46871	CVE-2023-21840	CVE-2023-25739
CVE-2022-24675	CVE-2022-30631	CVE-2022-3736	CVE-2022-46874	CVE-2023-21843	CVE-2023-25742
CVE-2022-24963	CVE-2022-30632	CVE-2022-37436	CVE-2022-46877	CVE-2023-21896	CVE-2023-25743
CVE-2022-25147	CVE-2022-30633	CVE-2022-38171	CVE-2022-48281	CVE-2023-21928	CVE-2023-25744
CVE-2022-25255	CVE-2022-30634	CVE-2022-38784	CVE-2023-0215	CVE-2023-21984	CVE-2023-25746
CVE-2022-27337	CVE-2022-30635	CVE-2022-3924	CVE-2023-0216	CVE-2023-21985	CVE-2023-25751
CVE-2022-27536	CVE-2022-3094	CVE-2022-39253	CVE-2023-0217	CVE-2023-22003	CVE-2023-25752
CVE-2022-27664	CVE-2022-3099	CVE-2022-40303	CVE-2023-0286	CVE-2023-22490	CVE-2023-27522
CVE-2022-27778	CVE-2022-3134	CVE-2022-40304	CVE-2023-0401	CVE-2023-22809	CVE-2023-28162
CVE-2022-28131	CVE-2022-3153	CVE-2022-40898	CVE-2023-0411	CVE-2023-23598	CVE-2023-28163
CVE-2022-2816	CVE-2022-32148	CVE-2022-41715	CVE-2023-0412	CVE-2023-23599	CVE-2023-28164
CVE-2022-2817	CVE-2022-32189	CVE-2022-41716	CVE-2023-0413	CVE-2023-23601	CVE-2023-28176
CVE-2022-2819	CVE-2022-32190	CVE-2022-41903	CVE-2023-0414	CVE-2023-23602	CVE-2023-28708
CVE-2022-28327	CVE-2022-32205	CVE-2022-42010	CVE-2023-0415	CVE-2023-23603	
CVE-2022-28331	CVE-2022-32206	CVE-2022-42011	CVE-2023-0416	CVE-2023-23605	
CVE-2022-2845	CVE-2022-32207	CVE-2022-42012	CVE-2023-0417	CVE-2023-23918	
CVE-2022-2849	CVE-2022-32208	CVE-2022-4203	CVE-2023-0430	CVE-2023-23919	
CVE-2022-2862	CVE-2022-32221	CVE-2022-4283	CVE-2023-0567	CVE-2023-23920	

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 April 2023 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.k4.85.S11 and 93.M3.14 software releases. We have not tested the April 2023 Security Patch Cluster on all earlier FreeFlow® Print Server 9.3 releases, but there should not be any problems on these releases.

The April 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, 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:	11.4.56.138.2
FFPS Release Version	9.0_SP-3_(93.M3.14.86)
FFPS Patch Cluster	April 2023
Java Version	Java 7 Update 331
Base Repository	Installed
Firefox Version	102.9.0esr
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

The above versions are the correct information after installing the April 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 April 2023 Security Patch Cluster includes a ZIP and ISO image file. The ISO image file can be written to DVD media to transport and install on the FreeFlow® Print Server platform. The ZIP file can be copied 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 April 2023 Security Patch Cluster can be installed from USB/DVD 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 illustrate file size on Windows®, file size on Solaris® and checksum on Solaris® for the April 2023 Security Patch Cluster files.

April 2023 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Apr2023SecurityPatches_v9S11_4-Part1.zip	3,935,139	4,029,581,328	58821 7870277
Apr2023SecurityPatches_v9S11_4-Part2.zip	4,183,320	4,283,719,025	41856 8366639
Apr2023SecurityPatches_v9S11_4-Part3.zip	3,536,498	3,621,373,256	20537 7072995
Apr2023SecurityPatches_v9S11_4-Part4.zip	4,101,676	4,200,115,924	5539 8203352

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 **Apr2023SecurityPatches_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