Xerox Security Bulletin XRX22-014

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 2022 Security Patch Cluster
Includes: N/A
Bulletin Date: June 20, 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. **April 2022 Security Patch Cluster**
   - Supersedes January 2022 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 311 Software.
3. **Firefox 91.7.0esr Software**
   - Supersedes Firefox 91.4.0esr

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v91.7.0esr software below:

Firefox v91.7.0esr Software Remediated US-CERT CVE's					
CVE-2021-4140	CVE-2022-22741	CVE-2022-22746	CVE-2022-22754	CVE-2022-22763	CVE-2022-26386
CVE-2022-22737	CVE-2022-22742	CVE-2022-22747	CVE-2022-22756	CVE-2022-22764	CVE-2022-26387
CVE-2022-22738	CVE-2022-22743	CVE-2022-22748	CVE-2022-22759	CVE-2022-26381	CVE-2022-26485
CVE-2022-22739	CVE-2022-22744	CVE-2022-22751	CVE-2022-22760	CVE-2022-26383	CVE-2022-26486
CVE-2022-22740	CVE-2022-22745	CVE-2022-22753	CVE-2022-22761	CVE-2022-26384	

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

April 2022 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2016-2124	CVE-2021-3875	CVE-2021-4182	CVE-2021-45078	CVE-2022-21416	CVE-2022-22763
CVE-2019-14822	CVE-2021-3903	CVE-2021-4183	CVE-2021-45115	CVE-2022-21446	CVE-2022-22764
CVE-2019-19906	CVE-2021-39212	CVE-2021-4184	CVE-2021-45116	CVE-2022-21461	CVE-2022-22764
CVE-2020-15250	CVE-2021-39272	CVE-2021-4185	CVE-2021-45452	CVE-2022-21463	CVE-2022-22815
CVE-2020-17049	CVE-2021-3928	CVE-2021-42717	CVE-2021-45960	CVE-2022-21493	CVE-2022-22816
CVE-2020-25717	CVE-2021-3968	CVE-2021-42762	CVE-2021-46143	CVE-2022-21494	CVE-2022-22817
CVE-2020-25718	CVE-2021-3973	CVE-2021-43331	CVE-2022-0336	CVE-2022-21712	CVE-2022-22818
CVE-2020-25719	CVE-2021-3974	CVE-2021-43332	CVE-2022-0391	CVE-2022-21716	CVE-2022-22822
CVE-2020-25721	CVE-2021-3984	CVE-2021-43395	CVE-2022-0566	CVE-2022-21824	CVE-2022-22823
CVE-2020-25722	CVE-2021-39920	CVE-2021-43527	CVE-2022-0581	CVE-2022-22719	CVE-2022-22824
CVE-2020-9484	CVE-2021-39921	CVE-2021-43528	CVE-2022-0582	CVE-2022-22720	CVE-2022-22825
CVE-2021-21707	CVE-2021-39922	CVE-2021-43536	CVE-2022-0583	CVE-2022-22721	CVE-2022-22826
CVE-2021-22926	CVE-2021-39923	CVE-2021-43537	CVE-2022-0585	CVE-2022-22737	CVE-2022-22827
CVE-2021-23192	CVE-2021-39924	CVE-2021-43538	CVE-2022-0586	CVE-2022-22738	CVE-2022-23181
CVE-2021-27815	CVE-2021-39925	CVE-2021-43539	CVE-2022-0778	CVE-2022-22739	CVE-2022-23833
CVE-2021-30846	CVE-2021-39926	CVE-2021-43541	CVE-2022-21248	CVE-2022-22740	CVE-2022-23852
CVE-2021-30848	CVE-2021-39928	CVE-2021-43542	CVE-2022-21263	CVE-2022-22741	CVE-2022-23943
CVE-2021-30849	CVE-2021-39929	CVE-2021-43543	CVE-2022-21271	CVE-2022-22742	CVE-2022-23990
CVE-2021-30851	CVE-2021-4008	CVE-2021-43545	CVE-2022-21282	CVE-2022-22743	CVE-2022-24407
CVE-2021-30858	CVE-2021-4009	CVE-2021-43546	CVE-2022-21291	CVE-2022-22744	CVE-2022-25235
CVE-2021-33430	CVE-2021-4010	CVE-2021-43566	CVE-2022-21293	CVE-2022-22744	CVE-2022-25236
CVE-2021-34141	CVE-2021-4011	CVE-2021-43818	CVE-2022-21294	CVE-2022-22745	CVE-2022-25313
CVE-2021-35604	CVE-2021-40145	CVE-2021-44142	CVE-2022-21296	CVE-2022-22746	CVE-2022-25314
CVE-2021-35624	CVE-2021-4019	CVE-2021-44224	CVE-2022-21298	CVE-2022-22746	CVE-2022-25315
CVE-2021-3572	CVE-2021-4034	CVE-2021-44227	CVE-2022-21299	CVE-2022-22747	CVE-2022-26381
CVE-2021-3711	CVE-2021-4069	CVE-2021-44420	CVE-2022-21305	CVE-2022-22748	CVE-2022-26383
CVE-2021-3733	CVE-2021-40812	CVE-2021-44531	CVE-2022-21340	CVE-2022-22751	CVE-2022-26384
CVE-2021-3737	CVE-2021-41133	CVE-2021-44532	CVE-2022-21341	CVE-2022-22753	CVE-2022-26386
CVE-2021-3738	CVE-2021-4140	CVE-2021-44533	CVE-2022-21349	CVE-2022-22754	CVE-2022-26387
CVE-2021-3770	CVE-2021-41495	CVE-2021-44540	CVE-2022-21360	CVE-2022-22756	CVE-2022-26387
CVE-2021-3778	CVE-2021-41496	CVE-2021-44541	CVE-2022-21365	CVE-2022-22759	CVE-2022-26485
CVE-2021-3796	CVE-2021-4181	CVE-2021-44542	CVE-2022-21365	CVE-2022-22760	CVE-2022-26486
CVE-2021-38115	CVE-2021-41817	CVE-2021-44543	CVE-2022-21375	CVE-2022-22761	
CVE-2021-3872	CVE-2021-41819	CVE-2021-44790	CVE-2022-21384	CVE-2022-22761	

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/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 April 2022 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 software release. We have not tested the April 2022 Security Patch Cluster on all earlier FreeFlow® Print Server 9.3 releases, but there should not be any problems on these releases.

The April 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, 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
FFPS Release Version	9.0_SP-3_(93.k4.85.86)
FFPS Patch Cluster	April 2022
Java Version	Java 7 Update 331
Base Repository	Installed
Firefox Version	91.7.0esr
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

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

April 2022 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Apr2022SecurityPatches_v9S11_4-Part1.zip	3,603,047	3,689,519,374	50073 7206093
Apr2022SecurityPatches_v9S11_4-Part2.zip	3,571,555	3,657,271,700	59242 7143109
Apr2022SecurityPatches_v9S11_4-Part3.zip	3,502,668	3,586,731,072	15779 7005335
Apr2022SecurityPatches_v9S11_4-Part4.zip	3,387,243	3,468,536,718	5420 6774486

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 **Apr2022SecurityPatches_v9S11.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