Xerox Security Bulletin XRX22-021

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: July 2022 Security Patch Cluster
Includes: N/A
Bulletin Date: September 6, 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. **July 2022 Security Patch Cluster**
   - Supersedes April 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 91.10.0esr Software**
   - Supersedes Firefox 91.7.0esr

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v91.10.0esr software below:

Firefox v91.10.0esr Software Remediated US-CERT CVE's					
CVE-2022-1097	CVE-2022-28282	CVE-2022-29909	CVE-2022-29916	CVE-2022-31738	CVE-2022-31742
CVE-2022-1196	CVE-2022-28285	CVE-2022-29911	CVE-2022-29917	CVE-2022-31739	CVE-2022-31747
CVE-2022-24713	CVE-2022-28286	CVE-2022-29912	CVE-2022-31736	CVE-2022-31740	
CVE-2022-28281	CVE-2022-28289	cVE-2022-29914	CVE-2022-31737	CVE-2022-31741	

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

July 2022 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2018-25032	CVE-2021-3448	CVE-2022-0319	CVE-2022-21367	CVE-2022-22827	CVE-2022-28281
CVE-2019-19906	CVE-2021-34558	CVE-2022-0336	CVE-2022-21426	CVE-2022-23308	CVE-2022-28282
CVE-2020-0499	CVE-2021-36221	CVE-2022-0391	CVE-2022-21434	CVE-2022-23772	CVE-2022-28285
CVE-2020-25717	CVE-2021-4115	CVE-2022-0408	CVE-2022-21443	CVE-2022-23773	CVE-2022-28286
CVE-2020-29651	CVE-2021-4136	CVE-2022-0413	CVE-2022-21449	CVE-2022-23806	CVE-2022-28289
CVE-2021-0561	CVE-2021-4166	CVE-2022-0417	CVE-2022-21476	CVE-2022-23833	CVE-2022-28327
CVE-2021-21708	CVE-2021-4173	CVE-2022-0443	CVE-2022-21493	CVE-2022-23852	CVE-2022-28346
CVE-2021-22946	CVE-2021-41771	CVE-2022-0554	CVE-2022-21494	CVE-2022-23943	CVE-2022-28347
CVE-2021-25220	CVE-2021-41772	CVE-2022-0566	CVE-2022-21496	CVE-2022-23990	CVE-2022-29824
CVE-2021-29923	CVE-2021-4187	CVE-2022-0572	CVE-2022-21514	CVE-2022-24130	CVE-2022-29909
CVE-2021-30809	CVE-2021-4192	CVE-2022-0629	CVE-2022-21524	CVE-2022-24407	CVE-2022-29911
CVE-2021-30818	CVE-2021-4193	CVE-2022-0685	CVE-2022-21533	CVE-2022-24675	CVE-2022-29912
CVE-2021-30823	CVE-2021-4217	CVE-2022-0696	CVE-2022-21712	CVE-2022-24713	CVE-2022-29913
CVE-2021-30836	CVE-2021-43519	CVE-2022-0714	CVE-2022-21716	CVE-2022-24801	CVE-2022-29914
CVE-2021-30884	CVE-2021-43566	CVE-2022-0729	CVE-2022-22589	CVE-2022-25235	CVE-2022-29916
CVE-2021-30887	CVE-2021-44142	CVE-2022-0778	CVE-2022-22590	CVE-2022-25236	CVE-2022-29917
CVE-2021-30888	CVE-2021-45444	CVE-2022-1097	CVE-2022-22592	CVE-2022-25313	CVE-2022-31736
CVE-2021-30889	CVE-2021-45481	CVE-2022-1196	CVE-2022-22620	CVE-2022-25314	CVE-2022-31737
CVE-2021-30890	CVE-2021-45482	CVE-2022-1197	CVE-2022-22719	CVE-2022-25315	CVE-2022-31738
CVE-2021-30897	CVE-2021-45483	CVE-2022-1271	CVE-2022-22720	CVE-2022-25762	CVE-2022-31739
CVE-2021-30934	CVE-2021-45960	CVE-2022-1520	CVE-2022-22721	CVE-2022-26381	CVE-2022-3174
CVE-2021-30936	CVE-2021-46143	CVE-2022-1834	CVE-2022-22818	CVE-2022-26383	CVE-2022-31740
CVE-2021-30951	CVE-2022-0128	CVE-2022-21245	CVE-2022-22822	CVE-2022-26384	CVE-2022-31741
CVE-2021-30952	CVE-2022-0156	CVE-2022-21270	CVE-2022-22823	CVE-2022-26386	CVE-2022-31742
CVE-2021-30953	CVE-2022-0158	CVE-2022-21303	CVE-2022-22824	CVE-2022-26387	CVE-2022-31747
CVE-2021-30954	CVE-2022-0261	CVE-2022-21304	CVE-2022-22825	CVE-2022-26485	CVE-2022-4187
CVE-2021-30984	CVE-2022-0318	CVE-2022-21344	CVE-2022-22826	CVE-2022-26486	CVE-2022-28281

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 July 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 July 2022 Security Patch Cluster on all earlier FreeFlow® Print Server 9.3 releases, but there should not be any problems on these releases.

The July 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	July 2022
Java Version	Java 7 Update 331
Base Repository	Installed
Firefox Version	91.10.0esr
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

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

July 2022 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jul2022SecurityPatches_v9S11_4-Part1.zip	3,529,248	3,613,948,983	20762 7058495
Jul2022SecurityPatches_v9S11_4-Part2.zip	3,744,458	3,834,324,210	40276 7488915
Jul2022SecurityPatches_v9S11_4-Part3.zip	3,377,696	3,458,760,087	40856 6755391
Jul2022SecurityPatches_v9S11_4-Part4.zip	3,688,232	3,445,722,273	28396 6729927

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 **Jul2022SecurityPatches_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