Xerox Security Bulletin XRX23-011

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: July 2023 Security Patch Cluster
Includes: Apache 2.4.57 and Firefox 102.12.0.esr Software
Bulletin Date: August 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. **July 2023 Security Patch Cluster**
   - Supersedes April 2023 Security Patch Cluster
   - This Patch Cluster is only intended for FFPS 73.M1.90 / RV 14.4.28 software. You will first have to perform a software scrape to this release (or later) before installing the July 2023 Security Patch Cluster.
2. **OpenJDK 8 Update 382-b09 Software**
   - Supersedes the OpenJDK 8 Update 372-b07 Software.
3. **Apache 2.4.57 Software**
   - Same version that was available in the April 2023 Security Patch Cluster.
4. **Firefox 102.12.0esr Software**
   - Supersedes Firefox 102.9.0esr Software.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v102.12.0esr software below:

Firefox v102.12.0esr Software Remediated US-CERT CVE's					
CVE-2023-1945	CVE-2023-29535	CVE-2023-29542	CVE-2023-32205	CVE-2023-32212	CVE-2023-34414
CVE-2023-29531	CVE-2023-29536	CVE-2023-29545	CVE-2023-32206	CVE-2023-32213	CVE-2023-34416
CVE-2023-29532	CVE-2023-29539	CVE-2023-29548	CVE-2023-32207	CVE-2023-32214	
CVE-2023-29533	CVE-2023-29541	CVE-2023-29550	CVE-2023-32211	CVE-2023-32215	

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 382-b09 software below:

OpenJDK 8 Update 382-b09 Software Remediated US-CERT CVE's			
CVE-2023-22006	CVE-2023-22041	CVE-2023-22045	CVE-2023-25193
CVE-2023-22036	CVE-2023-22044	CVE-2023-22049	

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 July 2023 Security Patch Cluster remediate in table below:

July 2023 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2004-0687	CVE-2022-37434	CVE-2022-4904	CVE-2023-21962	CVE-2023-26769	CVE-2023-29550
CVE-2020-23903	CVE-2022-39348	CVE-2023-0215	CVE-2023-21966	CVE-2023-2731	CVE-2023-30086
CVE-2020-23904	CVE-2022-40897	CVE-2023-0494	CVE-2023-21972	CVE-2023-27320	CVE-2023-30608
CVE-2021-33621	CVE-2022-41716	CVE-2023-0547	CVE-2023-21976	CVE-2023-28484	CVE-2023-30774
CVE-2021-33657	CVE-2022-41717	CVE-2023-1161	CVE-2023-21977	CVE-2023-28486	CVE-2023-30775
CVE-2021-3575	CVE-2022-41720	CVE-2023-1945	CVE-2023-21980	CVE-2023-28487	CVE-2023-31047
CVE-2021-3618	CVE-2022-41722	CVE-2023-1992	CVE-2023-21982	CVE-2023-28709	CVE-2023-31284
CVE-2021-43618	CVE-2022-41723	CVE-2023-1993	CVE-2023-21995	CVE-2023-28755	CVE-2023-32205
CVE-2022-2097	CVE-2022-41724	CVE-2023-1994	CVE-2023-22023	CVE-2023-28756	CVE-2023-32206
CVE-2022-21123	CVE-2022-41725	CVE-2023-1999	CVE-2023-23931	CVE-2023-29007	CVE-2023-32207
CVE-2022-21125	CVE-2022-42898	CVE-2023-21911	CVE-2023-24021	CVE-2023-29400	CVE-2023-32211
CVE-2022-21127	CVE-2022-42916	CVE-2023-21912	CVE-2023-24532	CVE-2023-29469	CVE-2023-32212
CVE-2022-21166	CVE-2022-43551	CVE-2023-21919	CVE-2023-24534	CVE-2023-29479	CVE-2023-32213
CVE-2022-21589	CVE-2022-43552	CVE-2023-21920	CVE-2023-24536	CVE-2023-29531	CVE-2023-32214
CVE-2022-21592	CVE-2022-44617	CVE-2023-21929	CVE-2023-24537	CVE-2023-29532	CVE-2023-32215
CVE-2022-21608	CVE-2022-44792	CVE-2023-21933	CVE-2023-24538	CVE-2023-29533	CVE-2023-32324
CVE-2022-21617	CVE-2022-44793	CVE-2023-21935	CVE-2023-24539	CVE-2023-29535	CVE-2023-34414
CVE-2022-28805	CVE-2022-46285	CVE-2023-21940	CVE-2023-24540	CVE-2023-29536	CVE-2023-34416
CVE-2022-30115	CVE-2022-46663	CVE-2023-21945	CVE-2023-24998	CVE-2023-29539	CVE-2023-34981
CVE-2022-31783	CVE-2022-46908	CVE-2023-21946	CVE-2023-25652	CVE-2023-29541	
CVE-2022-33099	CVE-2022-4743	CVE-2023-21947	CVE-2023-25815	CVE-2023-29542	
CVE-2022-3729	CVE-2022-48303	CVE-2023-21953	CVE-2023-26767	CVE-2023-29545	
CVE-2022-37290	CVE-2022-4883	CVE-2023-21955	CVE-2023-26768	CVE-2023-29548	

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

The July 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:	11.4.59.144.2
FFPS Release Version	7.0_SP-3 (73.M1.90.11.86)
FFPS Patch Cluster	July 2023
Java Version	OpenJDK 8 Update 382
Base Repository	Installed
Firefox Version	102.12.0esr
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

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

July 2023 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jul2023AndOpenJDK8Update382Patches_v7S11_4-Part1.zip	4019841	4116316327	21672 8039681
Jul2023AndOpenJDK8Update382Patches_v7S11_4-Part2.zip	4480445	4587974737	53054 8960889
Jul2023AndOpenJDK8Update382Patches_v7S11_4-Part3.zip	3733321	3822920504	52902 7466642
Jul2023AndOpenJDK8Update382Patches_v7S11_4-Part4.zip	4136622	4235900040	15628 8273243

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 Jul2023AndOpenJDK8Update382Patches_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.