Xerox Security Bulletin XRX24-017

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 2024 Security Patch Cluster
Includes: Apache HTTP 2.4.62, Apache Tomcat 8.5.100, OpenSSL 1.0.2Zj, OpenSSH 9.6p1 and Firefox 115.12.0esr Software
Bulletin Date: November 18, 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 authorizes 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 2024 Security Patch Cluster**
   - Supersedes April 2024 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 HTTP 2.4.62 Software**
   - Supersedes Apache HTTP 2.4.59 Software.
4. **Apache Tomcat 8.5.100 Software**
   - Supersedes Tomcat 8.5.99 software
5. **Firefox 115.12.0esr Software**
   - Supersedes Firefox 102.15.0esr Software.
6. **OpenSSL 1.0.2.zj Software**
   - Supersedes OpenSSL 1.0.2.zi Software
7. **OpenSSH 9.6p1 Software**
   - Same as delivered with previous April 2024 Security Patch Cluster.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v115.12.0esr software below:

Firefox v115.12.0esr Software Remediated US-CERT CVE's					
CVE-2024-2609	CVE-2024-3857	CVE-2024-3864	CVE-2024-4769	CVE-2024-5690	CVE-2024-5696
CVE-2024-3302	CVE-2024-3859	CVE-2024-4367	CVE-2024-4770	CVE-2024-5691	CVE-2024-5700
CVE-2024-3852	CVE-2024-3861	CVE-2024-4767	CVE-2024-4777	CVE-2024-5692	CVE-2024-5702
CVE-2024-3854	CVE-2024-3863	CVE-2024-4768	CVE-2024-5688	CVE-2024-5693	

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 HTTP 2.4.62 software below:

Apache HTTP 2.4.62 Remediated US-CERT CVE's					
CVE-2024-36387	CVE-2024-38473	CVE-2024-38474	CVE-2024-38476	CVE-2024-39884	CVE-2024-40725
CVE-2024-38472	CVE-2024-39573	CVE-2024-38475	CVE-2024-38477	CVE-2024-40898	

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache Tomcat 8.5.100 software below:

Apache Tomcat 8.5.100 Software Remediated US-CERT CVE's			
N/A			

Note: There are no CVE findings for the Apache Tomcat update. This new software includes bug fixes.

See the US-CERT Common Vulnerability Exposures (CVE) the July 2024 Security Patch Cluster remediate in table below:

July 2024 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2015-2809	CVE-2023-46218	CVE-2024-0690	CVE-2024-20984	CVE-2024-2609	CVE-2024-3857
CVE-2017-6519	CVE-2023-46219	CVE-2024-0853	CVE-2024-20985	CVE-2024-26256	CVE-2024-3859
CVE-2018-6952	CVE-2023-46852	CVE-2024-0911	CVE-2024-20994	CVE-2024-27280	CVE-2024-3861
CVE-2019-20633	CVE-2023-46853	CVE-2024-1013	CVE-2024-20998	CVE-2024-27281	CVE-2024-3863
CVE-2021-45261	CVE-2023-48795	CVE-2024-1931	CVE-2024-21000	CVE-2024-27282	CVE-2024-3864
CVE-2022-31629	CVE-2023-49355	CVE-2024-2002	CVE-2024-21008	CVE-2024-27316	CVE-2024-4340
CVE-2022-33065	CVE-2023-50246	CVE-2024-20697	CVE-2024-21009	CVE-2024-27351	CVE-2024-4367
CVE-2022-37026	CVE-2023-50268	CVE-2024-20960	CVE-2024-21013	CVE-2024-2756	CVE-2024-4577
CVE-2022-47069	CVE-2023-50269	CVE-2024-20961	CVE-2024-21047	CVE-2024-2757	CVE-2024-4767
CVE-2023-31102	CVE-2023-50387	CVE-2024-20962	CVE-2024-21054	CVE-2024-27982	CVE-2024-4768
CVE-2023-36054	CVE-2023-50868	CVE-2024-20963	CVE-2024-21060	CVE-2024-27982	CVE-2024-4769
CVE-2023-37920	CVE-2023-51764	CVE-2024-20964	CVE-2024-21062	CVE-2024-27983	CVE-2024-4770
CVE-2023-38469	CVE-2023-52425	CVE-2024-20965	CVE-2024-21069	CVE-2024-27983	CVE-2024-4777
CVE-2023-38470	CVE-2023-52426	CVE-2024-20966	CVE-2024-21087	CVE-2024-28219	CVE-2024-4853
CVE-2023-38471	CVE-2023-5341	CVE-2024-20967	CVE-2024-21096	CVE-2024-2955	CVE-2024-4854
CVE-2023-38472	CVE-2023-5363	CVE-2024-20969	CVE-2024-21151	CVE-2024-3096	CVE-2024-4855
CVE-2023-38473	CVE-2023-5678	CVE-2024-20970	CVE-2024-21885	CVE-2024-32002	CVE-2024-5458
CVE-2023-38709	CVE-2023-6129	CVE-2024-20971	CVE-2024-21886	CVE-2024-32004	CVE-2024-5585
CVE-2023-39975	CVE-2023-6237	CVE-2024-20972	CVE-2024-23638	CVE-2024-32020	CVE-2024-5688
CVE-2023-40481	CVE-2023-6597	CVE-2024-20973	CVE-2024-2408	CVE-2024-32021	CVE-2024-5691
CVE-2023-41993	CVE-2023-6816	CVE-2024-20974	CVE-2024-24258	CVE-2024-32465	CVE-2024-5692
CVE-2023-42465	CVE-2023-7104	CVE-2024-20975	CVE-2024-24259	CVE-2024-3302	CVE-2024-5693
CVE-2023-4408	CVE-2023-7250	CVE-2024-20976	CVE-2024-24783	CVE-2024-33655	CVE-2024-5696
CVE-2023-45288	CVE-2024-0229	CVE-2024-20977	CVE-2024-24784	CVE-2024-34064	CVE-2024-5700
CVE-2023-45289	CVE-2024-0408	CVE-2024-20978	CVE-2024-24785	CVE-2024-37407	CVE-2024-5702
CVE-2023-45290	CVE-2024-0409	CVE-2024-20981	CVE-2024-24795	CVE-2024-3852	
CVE-2023-46118	CVE-2024-0450	CVE-2024-20982	CVE-2024-25629	CVE-2024-3854	

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 installation 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 installation.

The July 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 July 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 July 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 installation.

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:	11.4.71.170.2
FFPS Release Version	9.0_SP-3_(93.M3.14.86)
FFPS Patch Cluster	July 2024
Java Version	Java 7 Update 331

The above versions are the correct information after installing the July 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 onto 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 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 installation. Alternatively, the July 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 July 2024 Security Patch Cluster files.

July 2024 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jul2024SecurityPatches_v9S11_4-Part1.zip	3,810,813	3,902,271,912	19345 7621625
Jul2024SecurityPatches_v9S11_4-Part2.zip	5,203,383	5,328,264,134	58089 10406766
Jul2024SecurityPatches_v9S11_4-Part3.zip	3,516,981	3,601,388,220	16905 7033962
Jul2024SecurityPatches_v9S11_4-Part4.zip	4,241,572	4,343,369,152	18890 8483143

Verify integrity of the Security Patch files from the FreeFlow® Print Server hard drive by comparing the actual checksum (using UNIX 'sum' command) of these files copied to the platform with the Solaris checksum in the above table. Change directory to the directory location where the Security Patch Cluster file was copied and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., **sum Jul2024SecurityPatches_v9S11_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 a 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.