Xerox Security Bulletin XRX25-001

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: October 2024 Security Patch Cluster
Includes: Apache HTTP 2.4.62, Apache Tomcat 8.5.100, OpenSSL 1.0.2Zj, OpenSSH 9.6p1 and Firefox 128.2.0esr Software
Bulletin Date: January 9, 2025

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. **October 2024 Security Patch Cluster**
   - Supersedes July 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**
   - Same as delivered with previous July 2024 Security Patch Cluster.
4. **Apache Tomcat 8.5.100 Software**
   - Same as delivered with previous July 2024 Security Patch Cluster.
5. **Firefox 128.2.0esr Software**
   - Supersedes Firefox 115.12.0esr Software.
6. **OpenSSL 1.0.2.zj Software**
   - Same as delivered with previous July 2024 Security Patch Cluster.
7. **OpenSSH 9.6p1 Software**
   - Same as delivered with previous July 2024 Security Patch Cluster.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v128.2.0esr software below:

Firefox v128.2.0esr Software Remediated US-CERT CVE's					
CVE-2024-6600	CVE-2024-6606	CVE-2024-6612	CVE-2024-7520	CVE-2024-7527	CVE-2024-8383
CVE-2024-6601	CVE-2024-6607	CVE-2024-6613	CVE-2024-7521	CVE-2024-7528	CVE-2024-8384
CVE-2024-6602	CVE-2024-6608	CVE-2024-6614	CVE-2024-7522	CVE-2024-7529	CVE-2024-8385
CVE-2024-6603	CVE-2024-6609	CVE-2024-6615	CVE-2024-7524	CVE-2024-7531	CVE-2024-8386
CVE-2024-6604	CVE-2024-6610	CVE-2024-7518	CVE-2024-7525	CVE-2024-8381	CVE-2024-8387
CVE-2024-6605	CVE-2024-6611	CVE-2024-7519	CVE-2024-7526	CVE-2024-8382	CVE-2024-8383

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

October 2024 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2019-12900	CVE-2024-0397	CVE-2024-2466	CVE-2024-33869	CVE-2024-41989	CVE-2024-6615
CVE-2019-13232	CVE-2024-0553	CVE-2024-24787	CVE-2024-33870	CVE-2024-41990	CVE-2024-7518
CVE-2021-20251	CVE-2024-0567	CVE-2024-24788	CVE-2024-33871	CVE-2024-41991	CVE-2024-7519
CVE-2021-4209	CVE-2024-0760	CVE-2024-24789	CVE-2024-34750	CVE-2024-42005	CVE-2024-7520
CVE-2021-44141	CVE-2024-1737	CVE-2024-24790	CVE-2024-35195	CVE-2024-42353	CVE-2024-7521
CVE-2022-0529	CVE-2024-1975	CVE-2024-24791	CVE-2024-36137	CVE-2024-4453	CVE-2024-7522
CVE-2022-0530	CVE-2024-2004	CVE-2024-2511	CVE-2024-36138	CVE-2024-45230	CVE-2024-7525
CVE-2022-32742	CVE-2024-20996	CVE-2024-25111	CVE-2024-36387	CVE-2024-45231	CVE-2024-7526
CVE-2022-32744	CVE-2024-21125	CVE-2024-25580	CVE-2024-37372	CVE-2024-4603	CVE-2024-7527
CVE-2022-32745	CVE-2024-21127	CVE-2024-26306	CVE-2024-37891	CVE-2024-4741	CVE-2024-7528
CVE-2022-32746	CVE-2024-21129	CVE-2024-27980	CVE-2024-38286	CVE-2024-5197	CVE-2024-7529
CVE-2022-37966	CVE-2024-21130	CVE-2024-28182	CVE-2024-38472	CVE-2024-5569	CVE-2024-8381
CVE-2022-38023	CVE-2024-21134	CVE-2024-28757	CVE-2024-38473	CVE-2024-6197	CVE-2024-8382
CVE-2023-0361	CVE-2024-21142	CVE-2024-28834	CVE-2024-38474	CVE-2024-6600	CVE-2024-8384
CVE-2023-3347	CVE-2024-21147	CVE-2024-28835	CVE-2024-38475	CVE-2024-6601	CVE-2024-8385
CVE-2023-34966	CVE-2024-21162	CVE-2024-29510	CVE-2024-38477	CVE-2024-6602	CVE-2024-8386
CVE-2023-34967	CVE-2024-21163	CVE-2024-30161	CVE-2024-38875	CVE-2024-6603	CVE-2024-8387
CVE-2023-34968	CVE-2024-21165	CVE-2024-30202	CVE-2024-39329	CVE-2024-6604	CVE-2024-8394
CVE-2023-37920	CVE-2024-21171	CVE-2024-30203	CVE-2024-39330	CVE-2024-6605	CVE-2024-8645
CVE-2023-38497	CVE-2024-21173	CVE-2024-30204	CVE-2024-39331	CVE-2024-6606	
CVE-2023-40030	CVE-2024-21177	CVE-2024-30205	CVE-2024-39573	CVE-2024-6607	
CVE-2023-4091	CVE-2024-21179	CVE-2024-31080	CVE-2024-39614	CVE-2024-6608	
CVE-2023-45918	CVE-2024-21520	CVE-2024-31081	CVE-2024-39884	CVE-2024-6609	
CVE-2023-46045	CVE-2024-22018	CVE-2024-31082	CVE-2024-39894	CVE-2024-6610	
CVE-2023-51714	CVE-2024-22020	CVE-2024-31083	CVE-2024-4032	CVE-2024-6611	
CVE-2023-52722	CVE-2024-22667	CVE-2024-31744	CVE-2024-40725	CVE-2024-6612	
CVE-2023-5388	CVE-2024-2379	CVE-2024-3205	CVE-2024-4076	CVE-2024-6613	
CVE-2023-5981	CVE-2024-2398	CVE-2024-32487	CVE-2024-40898	CVE-2024-6614	

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.

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 October 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 October 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 October 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:	11.4.74.176.3
FFPS Release Version	9.0_SP-3_(93.M3.14.86)
FFPS Patch Cluster	October 2024
Java Version	Java 7 Update 331

The above versions are the correct information after installing the October 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 October 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 October 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 October 2024 Security Patch Cluster files.

October 2024 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Oct2024SecurityPatches_v9S11_4-Part1.zip	3,651,255	3,738,884,759	19585 7302510
Oct2024SecurityPatches_v9S11_4-Part2.zip	5,439,076	5,569,612,981	24450 10878151
Oct2024SecurityPatches_v9S11_4-Part3.zip	3,733,668	3,823,275,505	25880 7467335
Oct2024SecurityPatches_v9S11_4-Part4.zip	3,905,266	3,998,991,602	53216 7810531

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 Oct2024SecurityPatches_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 of the foregoing limitation may not apply.