Xerox Security Bulletin XRX25-008

Xerox® FreeFlow® Print Server v7

For: Solaris® 11.4 Operating System
Install Method: Hard Disk / USB Media
Supports: Xerox Nuvera® PSIP RV 14.5 Printer Products

Deliverable: April 2025 Security Patch Cluster
Includes: OpenJDK 8 Update 452-b08, Apache HTTP 2.4.63, Apache Tomcat 8.5.100, OpenSSL 3.0.16, OpenSSH 9.6p1 and Firefox 128.8.0esr Software
Bulletin Date: May 8, 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. **April 2025 Security Patch Cluster**
   - Supersedes January 2025 Security Patch Cluster
   - This Patch Cluster is only intended for FFPS 73.M1.90 / RV 14.4.28, 73.N2.74 / RV 14.5.34 and FFPS 73.O3.81 / RV 14.5.36 software releases. If an earlier software release is installed it's recommended to first install the FFPS 73.O3.81 / RV 14.5.36 software release.
2. **OpenJDK 8 Update 452-b08 Software**
   - Supersedes Open JDK 8 Update 442-b05 Software.
3. **Apache HTTP 2.4.63 Software**
   - Same as delivered with previous January 2025 Security Patch Cluster.
4. **Apache Tomcat 8.5.100 Software**
   - Same as delivered with previous January 2025 Security Patch Cluster.
5. **Firefox 128.8.0esr Software**
   - Supersedes Firefox 128.5.0esr Software.
6. **OpenSSL 3.0.16 Software**
   - Supersedes OpenSSL 1.0.2.zj Software.
7. **OpenSSH 9.6p1 Software**
   - Same as delivered with previous January 2025 Security Patch Cluster.

Patch Cluster Caveats:

1. SFTP connection attempts to a Nuvera printer will fail if using weak encryption algorithms. The SFTP application must supports SHA2 hash and AES 512-bit stream encryption strengths or higher for connectivity with the Nuvera printer to be successful.

2. The April 2025 Security Patch Cluster breaks the IP Filtering feature for the IPv6 protocol. If you rely on the IP Filtering feature with IPv6, please submit an escalation to the Xerox hotline to get a fix for this issue.

See the US-CERT Common Vulnerability Exposures (CVE) the April 2025 Security Patch Cluster remediate in table below:

April 2025 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2015-1197	CVE-2024-11612	CVE-2024-45490	CVE-2024-52531	CVE-2025-0510	CVE-2025-1935
CVE-2016-1938	CVE-2024-11704	CVE-2024-45491	CVE-2024-52532	CVE-2025-0938	CVE-2025-1936
CVE-2017-10176	CVE-2024-12084	CVE-2024-45492	CVE-2024-52533	CVE-2025-1009	CVE-2025-1937
CVE-2017-13693	CVE-2024-12085	CVE-2024-45795	CVE-2024-54677	CVE-2025-1010	CVE-2025-1938
CVE-2017-13694	CVE-2024-12086	CVE-2024-45796	CVE-2024-56201	CVE-2025-1011	CVE-2025-22150
CVE-2017-7781	CVE-2024-12087	CVE-2024-45797	CVE-2024-56326	CVE-2025-1012	CVE-2025-22870
CVE-2018-12404	CVE-2024-12088	CVE-2024-46951	CVE-2024-56374	CVE-2025-1013	CVE-2025-23083
CVE-2019-11729	CVE-2024-12254	CVE-2024-46952	CVE-2024-56732	CVE-2025-1014	CVE-2025-23084
CVE-2020-11053	CVE-2024-12705	CVE-2024-46953	CVE-2024-6345	CVE-2025-1015	CVE-2025-23085
CVE-2020-12400	CVE-2024-12747	CVE-2024-46954	CVE-2024-8508	CVE-2025-1016	CVE-2025-23087
CVE-2020-6829	CVE-2024-13176	CVE-2024-46955	CVE-2024-9143	CVE-2025-1017	CVE-2025-23088
CVE-2022-21271	CVE-2024-20696	CVE-2024-46956	CVE-2024-9632	CVE-2025-1217	CVE-2025-23089
CVE-2023-1972	CVE-2024-34155	CVE-2024-47187	CVE-2024-9681	CVE-2025-1219	CVE-2025-24813
CVE-2023-20569	CVE-2024-34156	CVE-2024-47188	CVE-2025-0237	CVE-2025-1734	CVE-2025-26465
CVE-2023-49582	CVE-2024-34158	CVE-2024-47522	CVE-2025-0238	CVE-2025-1736	CVE-2025-26466
CVE-2023-6135	CVE-2024-36474	CVE-2024-48651	CVE-2025-0239	CVE-2025-1861	CVE-2025-27516
CVE-2023-7207	CVE-2024-39936	CVE-2024-48957	CVE-2025-0240	CVE-2025-1930	CVE-2025-30348
CVE-2023-7216	CVE-2024-42415	CVE-2024-48958	CVE-2025-0241	CVE-2025-1931	CVE-2025-30690
CVE-2024-11053	CVE-2024-43097	CVE-2024-49761	CVE-2025-0242	CVE-2025-1932	CVE-2025-30700
CVE-2024-11187	CVE-2024-45336	CVE-2024-50379	CVE-2025-0243	CVE-2025-1933	
CVE-2024-11235	CVE-2024-45341	CVE-2024-52530	CVE-2025-0509	CVE-2025-1934	

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.

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 452-b08 software below:

OpenJDK 8 Update 452-b08 Software Remediated US-CERT CVE's					
CVE-2025-21587	CVE-2025-30691	CVE-2025-30698			

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache HTTP 2.4.63 software below:

Apache HTTP 2.4.63 Remediated US-CERT CVE's					

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

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) list for the Firefox v128.8.0esr software below:

Firefox v128.8.0esr Software Remediated US-CERT CVE's					
CVE-2024-11704	CVE-2025-0240	CVE-2025-1010	CVE-2025-1016	CVE-2025-1933	CVE-2025-1938
CVE-2024-43097	CVE-2025-0241	CVE-2025-1011	CVE-2025-1017	CVE-2025-1934	
CVE-2025-0237	CVE-2025-0242	CVE-2025-1012	CVE-2025-1930	CVE-2025-1935	
CVE-2025-0238	CVE-2025-0243	CVE-2025-1013	CVE-2025-1931	CVE-2025-1936	
CVE-2025-0239	CVE-2025-1009	CVE-2025-1014	CVE-2025-1932	CVE-2025-1937	

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 April 2025 Security Patch Cluster is available for the FreeFlow® Print Server 73.N2.74 / RV 14.5.34 software release on the Solaris® 11.4 OS for the Nuvera® 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.N2.74.11 / RV 14.5.34 software release. Although it was not tested with the FreeFlow® Print Server 73.M1.90 / RV 14.4.28 software release, this release is supported, and the installation should be successful.

The April 2025 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:	11.4.80.189.2
FFPS Release Version	7.0_SP-3 (73.N2.74.11.86)
FFPS Patch Cluster	April 2025
Java Version	OpenJDK 8 Update 452

The above versions are the correct information after installing the April 2025 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 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 2025 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 April 2025 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 patches is corrupted 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 illustrates file size on Windows®, file size on Solaris® and checksum on Solaris® for the April 2025 Security Patch Cluster files.

April 2025 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Apr2025AndOpenJDK8Update452Patches_v7S11_4-Part1.zip	3,821,361	3,913,072,692	53319 7642721
Apr2025AndOpenJDK8Update452Patches_v7S11_4-Part2.zip	5,449,218	5,579,999,224	4282 10898436
Apr2025AndOpenJDK8Update452Patches_v7S11_4-Part3.zip	4,204,776	4,305,690,357	2791 8409552
Apr2025AndOpenJDK8Update452Patches_v7S11_4-Part4.zip	5,335,989	5,464,052,272	21836 10671978

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 Apr2025AndOpenJDK8Update452Patches_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 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.