

Xerox Security Bulletin XRX26-008

Xerox® FreeFlow® Print Server v9

For: Solaris® 11.4 Operating System

Supports: Xerox® Versant® 3100 Press

Deliverable: January 2026 Security Patch Cluster

Includes: Apache HTTP 2.4.66, Apache Tomcat 8.5.100, OpenSSL 3.0.18, OpenSSH 10.2p1 and Firefox 140.6.0esr Software

Bulletin Date: March 4, 2026

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. January 2026 Security Patch Cluster

- Supersedes October 2025 Security Patch Cluster

2. Java 7 Update 331

- Java updates are no longer supported for these printer products.
- Install the January 2022 Security Patch Cluster first if not already installed. It includes the Java 7 Update 331 Software.

3. Apache HTTP 2.4.66 Software

- Supersedes Apache HTTP 2.4.65 Software.

4. Apache Tomcat 8.5.100 Software

- Same as delivered with previous October 2025 Security Patch Cluster.

5. Firefox 140.6.0esr Software

- Supersedes Firefox 128.13.0esr Software.

6. OpenSSL 3.0.18 Software

- Supersedes OpenSSL 3.0.16 Software.

7. OpenSSH 10.2p1 Software

- Supersedes OpenSSH 10.0p2 Software.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v140.6.0esr software below:

Firefox v140.6.0esr Software Remediated US-CERT CVE's				
CVE-2025-14321	CVE-2025-14323	CVE-2025-14325	CVE-2025-14329	CVE-2025-14331
CVE-2025-14322	CVE-2025-14324	CVE-2025-14328	CVE-2025-14330	CVE-2025-14333

See the US-CERT Common Vulnerability Exposures (CVE) the January 2026 Security Patch Cluster remediate in table below:

January 2026 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2025-5994	CVE-2025-11411	CVE-2025-13945	CVE-2025-14324	CVE-2025-14331	CVE-2025-62168
CVE-2025-9640	CVE-2025-11626	CVE-2025-13946	CVE-2025-14325	CVE-2025-14333	CVE-2025-64460
CVE-2025-9817	CVE-2025-12105	CVE-2025-14321	CVE-2025-14328	CVE-2025-32728	
CVE-2025-10230	CVE-2025-13372	CVE-2025-14322	CVE-2025-14329	CVE-2025-61984	
CVE-2025-11021	CVE-2025-13499	CVE-2025-14323	CVE-2025-14330	CVE-2025-61985	

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 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 2.4.66 software below:

Apache HTTP 2.4.66 Remediated US-CERT CVE's				
CVE-2025-55753	CVE-2025-58098	CVE-2025-59775	CVE-2025-65082	CVE-2025-66200

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.

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.

This January 2026 Security Patch Update is available for the FreeFlow® Print Server v9 Software Release running on Solaris® v11.4 OS. The FreeFlow® Print Server software release tested with the January 2026 Security Patch Update installed per printer product is illustrated below:

Printer Products	Patch Update Tested Releases
Xerox® Versant® 3100 Press	FreeFlow® Print Server 93.M3.14

This Security patch deliverable has been tested on the FreeFlow® Print Server 93.M3.14 software release. We have not tested the January 2026 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 January 2026 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 April 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:	11.4.89.207.2
FFPS Release Version	9.0_SP-3_(93.M3.14.86)
FFPS Patch Cluster	January 2026
Java Version	Java 7 Update 331

The above versions are the correct information after installing the January 2026 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 January 2026 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 January 2026 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 January 2026 Security Patch Cluster files.

January 2026 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jan2026SecurityPatches_v9S11_4-Part1.zip	3,797,402	3,888,539,358	32375 7594804
Jan2026SecurityPatches_v9S11_4-Part2.zip	5,403,353	5,533,033,365	34658 10806706
Jan2026SecurityPatches_v9S11_4-Part3.zip	5,723,596	5,860,962,218	22039 11447192
Jan2026SecurityPatches_v9S11_4-Part4.zip	6,375,364	6,528,372,279	18302 12750728

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 Jan2026SecurityPatches_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.