Xerox Security Bulletin XRX26-015

Xerox® FreeFlow® Print Server v9

For: Solaris® 11.4 Operating System
Supports: Xerox® Versant® 3100 Press

Deliverable: July 2026 Security Patch Cluster
Includes: Apache HTTP 2.4.68, Apache Tomcat 8.5.100, OpenSSL 3.0.21, OpenSSH 10.3p1 and Firefox 140.11.0esr Software
Bulletin Date: September 29, 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. **July 2026 Security Patch Cluster**
   - Supersedes April 2026 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 2.4.68 Software**
   - Supersedes Apache HTTP 2.4.67 Software.
4. **Apache Tomcat 8.5.100 Software**
   - Same as delivered with previous April 2026 Security Patch Cluster.
5. **Firefox 140.11.0esr Software**
   - Supersedes Firefox 140.8.0esr Software.
6. **OpenSSL 3.0.21 Software**
   - Supersedes OpenSSL 3.0.19 Software.
7. **OpenSSH 10.3p1 Software**
   - Supersedes OpenSSH 10.2p1 Software.

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) the July 2026 Security Patch Cluster remediate in table below:

July 2026 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2025-14179	CVE-2026-34304	CVE-2026-42764	CVE-2026-50259	CVE-2026-6526	CVE-2026-7379
CVE-2026-1502	CVE-2026-34308	CVE-2026-42765	CVE-2026-50260	CVE-2026-6527	CVE-2026-7383
CVE-2026-21998	CVE-2026-35188	CVE-2026-42766	CVE-2026-50261	CVE-2026-6528	CVE-2026-7568
CVE-2026-22001	CVE-2026-35236	CVE-2026-42767	CVE-2026-50262	CVE-2026-6529	CVE-2026-8090
CVE-2026-22002	CVE-2026-35237	CVE-2026-42768	CVE-2026-50263	CVE-2026-6530	CVE-2026-8091
CVE-2026-22004	CVE-2026-35238	CVE-2026-42769	CVE-2026-50264	CVE-2026-6531	CVE-2026-8092
CVE-2026-22005	CVE-2026-35239	CVE-2026-42770	CVE-2026-5299	CVE-2026-6532	CVE-2026-8094
CVE-2026-22009	CVE-2026-35240	CVE-2026-42771	CVE-2026-5401	CVE-2026-6533	CVE-2026-8328
CVE-2026-22015	CVE-2026-39817	CVE-2026-42923	CVE-2026-5402	CVE-2026-6534	CVE-2026-8388
CVE-2026-22017	CVE-2026-39819	CVE-2026-42944	CVE-2026-5403	CVE-2026-6535	CVE-2026-8391
CVE-2026-29518	CVE-2026-39820	CVE-2026-42959	CVE-2026-5404	CVE-2026-6536	CVE-2026-8401
CVE-2026-32792	CVE-2026-39821	CVE-2026-42960	CVE-2026-5405	CVE-2026-6537	CVE-2026-8946
CVE-2026-33278	CVE-2026-39823	CVE-2026-43617	CVE-2026-5406	CVE-2026-6538	CVE-2026-8947
CVE-2026-33811	CVE-2026-39825	CVE-2026-43618	CVE-2026-5407	CVE-2026-6722	CVE-2026-8949
CVE-2026-33814	CVE-2026-39826	CVE-2026-43619	CVE-2026-5408	CVE-2026-6735	CVE-2026-8950
CVE-2026-33999	CVE-2026-39836	CVE-2026-43620	CVE-2026-5409	CVE-2026-6867	CVE-2026-8953
CVE-2026-34000	CVE-2026-40192	CVE-2026-44390	CVE-2026-5653	CVE-2026-6868	CVE-2026-8954
CVE-2026-34001	CVE-2026-40622	CVE-2026-44431	CVE-2026-5654	CVE-2026-6869	CVE-2026-8955
CVE-2026-34002	CVE-2026-41292	CVE-2026-44432	CVE-2026-5655	CVE-2026-6870	CVE-2026-8956
CVE-2026-34003	CVE-2026-41316	CVE-2026-44608	CVE-2026-5656	CVE-2026-7258	CVE-2026-8957
CVE-2026-34180	CVE-2026-42304	CVE-2026-45232	CVE-2026-5657	CVE-2026-7259	CVE-2026-8958
CVE-2026-34181	CVE-2026-42305	CVE-2026-45445	CVE-2026-6019	CVE-2026-7261	CVE-2026-8959
CVE-2026-34182	CVE-2026-42308	CVE-2026-45446	CVE-2026-6100	CVE-2026-7262	CVE-2026-8961
CVE-2026-34183	CVE-2026-42309	CVE-2026-45447	CVE-2026-6104	CVE-2026-7263	CVE-2026-8962
CVE-2026-34267	CVE-2026-42310	CVE-2026-46529	CVE-2026-6519	CVE-2026-7320	CVE-2026-8968
CVE-2026-34270	CVE-2026-42311	CVE-2026-47712	CVE-2026-6520	CVE-2026-7321	CVE-2026-8970
CVE-2026-34271	CVE-2026-42371	CVE-2026-47734	CVE-2026-6521	CVE-2026-7322	CVE-2026-8974
CVE-2026-34276	CVE-2026-42499	CVE-2026-4786	CVE-2026-6522	CVE-2026-7323	CVE-2026-8975
CVE-2026-34278	CVE-2026-42501	CVE-2026-50256	CVE-2026-6523	CVE-2026-7375	CVE-2026-9076
CVE-2026-34293	CVE-2026-42534	CVE-2026-50257	CVE-2026-6524	CVE-2026-7376	CVE-2026-9759
CVE-2026-34303	CVE-2026-42563	CVE-2026-50258	CVE-2026-6525	CVE-2026-7378	CVE-2026-7379

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 Apache HTTP 2.4.68 software below:

Apache HTTP 2.4.68 Remediated US-CERT CVE's				
CVE-2026-29167	CVE-2026-34356	CVE-2026-43951	CVE-2026-44186	CVE-2026-49975
CVE-2026-29170	CVE-2026-42535	CVE-2026-44119	CVE-2026-44631	
CVE-2026-34355	CVE-2026-42536	CVE-2026-44185	CVE-2026-48913	

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 v140.11.0esr software below:

Firefox v140.11.0esr Software Remediated US-CERT CVE's					
CVE-2026-7320	CVE-2026-8091	CVE-2026-8401	CVE-2026-8953	CVE-2026-8958	CVE-2026-8970
CVE-2026-7321	CVE-2026-8092	CVE-2026-8946	CVE-2026-8954	CVE-2026-8959	CVE-2026-8974
CVE-2026-7322	CVE-2026-8094	CVE-2026-8947	CVE-2026-8955	CVE-2026-8961	CVE-2026-8975
CVE-2026-7323	CVE-2026-8388	CVE-2026-8949	CVE-2026-8956	CVE-2026-8962	
CVE-2026-8090	CVE-2026-8391	CVE-2026-8950	CVE-2026-8957	CVE-2026-8968	

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 July 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 July 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 July 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 July 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:	11.4.94.221.2
FFPS Release Version	9.0_SP-3_(93.M3.14.86)
FFPS Patch Cluster	July 2026
Java Version	Java 7 Update 331

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

July 2026 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jul2026SecurityPatches_v9S11_4-Part1.zip	3,676,956	3,765,202,595	65280 7353912
Jul2026SecurityPatches_v9S11_4-Part2.zip	6,031,431	6,176,184,575	22540 12062861
Jul2026SecurityPatches_v9S11_4-Part3.zip	5,721,270	5,858,579,932	43393 11442539
Jul2026SecurityPatches_v9S11_4-Part4.zip	5,641,425	5,776,818,964	24464 11282850

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 Jul2026SecurityPatches_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.

© 2026 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design®, FreeFlow®, iGen®, Versant®, Brenva®, Impika®, and CiPress®, are trademarks of Xerox Corporation in the United States and/or other Countries. BR21127

Other company trademarks are also acknowledged.