

Xerox Security Bulletin XRX26-007

Xerox® FreeFlow® Print Server v2 / Windows® 10

Install Method: USB/DVD Media

Supports:

- Xerox® iGen®5 Press
- Xerox® Baltoro™ HF Production Inkjet Press

Deliverable: January 2026 Security Patch Update

Includes: OpenJDK Java 8 Update 482-b08, Apache HTTP 2.4.66, Apache Tomcat 6.0.45, OpenSSL 3.6.1, OpenSSH 10.0p2 and Firefox 147.0.2 Software

Bulletin Date: February 24, 2026

1.0 Background

Microsoft® responds to US CERT advisory council notifications of Security vulnerabilities referred to as Common Vulnerabilities and Exposures (CVE's) and develops patches that remediate the Security vulnerabilities that are applicable to Windows® 10 and components (e.g., Windows® Explorer®, .Net Framework®, etc.). The FreeFlow® Print Server organization has a dedicated development team, which actively review the US CERT advisory council CVE notifications, and delivers Security patch updates from Microsoft® to remediate the threat of these Security risks for the FreeFlow® Print Server v2 / Windows® v10 (supporting the Integrated and Standalone platforms)

The FreeFlow® Print Server organization delivers Security Patch Updates on the FreeFlow® Print Server v2 / Windows® v10 platform by the FreeFlow® Print Server organization on a quarterly basis. The FreeFlow® Print Server engineering team receives new patch updates in January, April, July, and October, and will test them for supported Printer products (such as iGen®5 printers) prior to delivery for customer install.

Xerox tests FreeFlow® Print Server operations with the patch updates to ensure there are no software issues prior to installing them at a customer location. Alternatively, a customer can use Windows® Update to install patch updates directly from Microsoft®. If the customer manages their own patch install, the Xerox support team can suggest options to minimize the risk of FreeFlow® Print Server operation problems that could result from patch updates.

This bulletin announces the availability of the following:

1. **January 2026 Security Patch Update**
 - This supersedes the October 2025 Security Patch Update.
2. **OpenJDK Java 8 Update 482-b08 Software**
 - This supersedes OpenJDK Java 8 Update 472-b08 Software.
3. **Firefox 147.0.2 Software**
 - This supersedes Firefox 144.0 Software.
4. **Apache HTTP 2.4.66 Software**
 - This supersedes Apache HTTP 2.4.65 Software.
5. **Apache Tomcat 6.0.45 Software**
 - Same as delivered with previous October 2025 Security Patch Update.
6. **OpenSSL 3.6.1 Software**
 - This supersedes OpenSSL 3.5.1 Software. OpenSSL is packaged with Apache software.
7. **Open SSH 10.0p2**
 - Same as delivered with previous October 2025 Security Patch Update.

Notice: The January 2026 Security Patch Update creates some noteworthy issues. The caveats after installing these Security patches are as follows:

1. SFTP connection attempts to a Xerox color press will fail if using weak encryption algorithms. If the SFTP application supports SHA2 hash and AES 512-bit stream encryption strengths connectivity will be successful.

Previously, the Xear Flex application was not able to connect to the printer using a secure FTP (SFTP) request. This application has now been updated with stronger encryption algorithms. Make sure you acquire the Xear Flex update to successfully connect to the printer with SFTP. The Security profile must be set to “High” for the secure connection to work successfully. It will not work with the “Low” Security profile.

2. The Security Profile set to the High option does not prevent access to the platform peripherals (E.g., DVD media, USB media, etc.).
3. The SNMPv3 service does not disable in the Security profile. This service is enabled by default with the built-in “High” profile. It is set to disable in the built-in “Low” and “Medium” profiles. The SNMPv3 service is available and responsive to incoming SNMP requests even though the current Security profile setting is disabled. The FFPS v24 post patches Baltoro_HF_24.0.24199.0_PATCH_BUNDLE_V2 (Baltoro Printer) and iGen_5_24.0.24199.0_PATCH_BUNDLE_V2 (iGen5 Printer) can be installed to fix this issue.

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

January 2026 Security Patch Update Remediated US-CERT CVE's					
CVE-2026-20804	CVE-2026-20822	CVE-2026-20834	CVE-2026-20849	CVE-2026-20875	CVE-2026-20931
CVE-2026-20805	CVE-2026-20823	CVE-2026-20836	CVE-2026-20852	CVE-2026-20919	CVE-2026-20932
CVE-2026-20809	CVE-2026-20824	CVE-2026-20839	CVE-2026-20853	CVE-2026-20921	CVE-2026-20934
CVE-2026-20812	CVE-2026-20826	CVE-2026-20840	CVE-2026-20856	CVE-2026-20922	CVE-2026-20936
CVE-2026-20814	CVE-2026-20827	CVE-2026-20843	CVE-2026-20860	CVE-2026-20925	CVE-2026-20937
CVE-2026-20816	CVE-2026-20828	CVE-2026-20844	CVE-2026-20868	CVE-2026-20926	CVE-2026-20939
CVE-2026-20820	CVE-2026-20831	CVE-2026-20847	CVE-2026-20869	CVE-2026-20927	CVE-2026-20940
CVE-2026-20821	CVE-2026-20832	CVE-2026-20848	CVE-2026-20872	CVE-2026-20929	CVE-2026-21265

Note: The official Microsoft® patches included in the January 2026 Security Patch Update are KB5073722, KB5073447 and KB890830.

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 482-b08software below:

OpenJDK 8 Update 482-b08 Remediated US-CERT CVE's					
CVE-2026-21925	CVE-2026-21932	CVE-2026-21933	CVE-2026-21945		

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 OpenSSL 3.6.1 software below:

OpenSSL 3.6.1 Software Remediated US-CERT CVE's				
N/A				

Note: There are no CVE's remediated in this OpenSSL 3.6.1 update. It only has bug fixes.

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox 147.0.2 software below:

Firefox 147.0.2 Software Remediated US-CERT CVE's					
CVE-2025-13012	CVE-2025-13021	CVE-2025-14323	CVE-2025-14332	CVE-2026-0880	CVE-2026-0889
CVE-2025-13013	CVE-2025-13022	CVE-2025-14324	CVE-2025-14333	CVE-2026-0881	CVE-2026-0890
CVE-2025-13014	CVE-2025-13023	CVE-2025-14325	CVE-2025-14860	CVE-2026-0882	CVE-2026-0891
CVE-2025-13015	CVE-2025-13024	CVE-2025-14326	CVE-2025-14861	CVE-2026-0883	CVE-2026-0892
CVE-2025-13016	CVE-2025-13025	CVE-2025-14327	CVE-2026-24868	CVE-2026-0884	
CVE-2025-13017	CVE-2025-13026	CVE-2025-14328	CVE-2026-24869	CVE-2026-0885	
CVE-2025-13018	CVE-2025-13027	CVE-2025-14329	CVE-2026-0877	CVE-2026-0886	
CVE-2025-13019	CVE-2025-14321	CVE-2025-14330	CVE-2026-0878	CVE-2026-0887	
CVE-2025-13020	CVE-2025-14322	CVE-2025-14331	CVE-2026-0879	CVE-2026-0888	

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 Update. The customer can manage their own Security Patch Updates using Windows® Update services, but we recommend checking with Xerox Service to reduce risk of installing patches that have not been tested by Xerox.

2.0 Applicability

This January 2026 Security Patch Update is available for the FreeFlow® Print Server v2 Software Release running on Windows® v10 OS. The FreeFlow® Print Server software release tested with the January 2026 Security Patch Update installed per printer products is illustrated below:

Printer Products	Patch Update Tested Releases
iGen®5 Press	CP.24.0.23126.0 / CP.24.0.24199.0
Baltoro™ HF Inkjet	CP.24.0.23126.0 / CP.24.0.24199.0

Although these January 2026 Security Patch Update was tested with the above FFPS v24 software release, there should be no problem installing on earlier software releases.

Security of the network, devices and information on a customer network may be a consideration when deciding whether to use the USB, or Windows® Update method of Security Patch Update delivery and install. Delivery and install of the Security Patch Update using Update Manager may still be a concern for some highly “secure” customer locations such as US Federal and State Government sites. Alternatively, delivery and installation of Security Patch Updates from USB media may be more desirable for these highly Security sensitive customers. They can perform a Security scan of the USB media with a virus protection application prior to install. If the customer does not allow use of USB media for devices on their network, you can transfer (using SMB, SFTP, or SCP) the Security Patch Update to the FreeFlow® Print Server platform, and then install.

3.0 Patch Install

Xerox strives to deliver these critical Security Patch Updates in a timely manner. The customer process to obtain FreeFlow® Print Server Security Patch Updates (delivered on a quarterly basis) is to contact the Xerox hotline support number. The methods of Security Patch Update delivery and install are over the network using FreeFlow® Print Server Update Manager or directly from Microsoft® using Windows® Update service, and using media (i.e., USB/DVD).

We recommend the customer use the FreeFlow® Print Server Update Manager or Microsoft® Windows® Update method if they wish to perform install on their own. This empowers the customer to have the option of installing these patch updates as soon as they become available, and not need to rely on the Xerox Service team. Many customers do not want the responsibility of installing the quarterly Security Patch Update or they are not comfortable providing a network tunnel to the Xerox or Microsoft® servers that store the Security Patch Update. In this case, the media install method is the best option under those circumstances.

3.1 USB/DVD Media Delivery

Xerox uploads the FreeFlow® Print Server Security Patch Update to a “secure” SFTP site that is available to the Xerox Analyst and Service once the deliverables have been tested and approved. The FreeFlow® Print Server patch deliverables are available as a ZIP archive, and a script used to perform the install. The Security Patch Update installs by executing a script and installs on top of a pre-installed FreeFlow® Print Server software release. The install script includes options to install the Security Patch Update directly from USB/DVD media or from the FreeFlow® Print Server internal hard disk. A PDF document is available with procedures to install the Security Patch Update using the USB/DVD media delivery method upon request.

If the Analyst supports their customer performing the Security Patch Update, then they must provide the customer with the Security Patch Update install document and the Security update deliverables. This method of Security Patch Update install is not as convenient or simple for customer install as the network install methods offered by Update Manger.

See the Security Patch Update deliverable filenames and sizes in the table below:

Security Patch File	Windows® Size (K-bytes)	Size in Bytes
FFPSv2-Win10_SecPatchUpdate_Jan2026.zip	2,260,857	2,315,116,661
FFPSv2-Win10_SecPatchUpdate_Jan2026.iso	2,261,208	2,315,476,992

3.2 Windows® Update Delivery

Windows® Update services enable information technology administrators to deploy the latest Microsoft® product updates to computers that are running the Windows® operating system. By using Windows® Update service, administrators can fully manage the distribution of updates released through Microsoft® Update to FreeFlow® Print Server platforms on their network.

Microsoft® uploads the Patch Updates to a server that is available on the Internet outside of the Microsoft® Corporate network once patch deliverables have been tested and approved. Installing the Security patches directly from Microsoft® using the Windows® Update service brings some risk given they have not been tested by Xerox on the FreeFlow® Print Server platform. It is required that the customer proxy server information be configured on the FreeFlow® Print Server platform so that the Windows® Update service can gain access to the Microsoft® server over the Internet outside of the customer network. Xerox is not responsible for the Security of the connection to the Microsoft® patch server.

We recommend manually performing a FreeFlow® Print Server System Backup and a Windows® Restore Point backup just prior to installing Windows® patch updates. This will ensure the FreeFlow® Print Server system recovery if the installed Security patches create a software problem or results in the FreeFlow® Print Server software becoming inoperable. The Security Patch Update makes changes to only the Windows® 10 OS system, and not the FreeFlow® Print Server software. Therefore, the restore of a Windows® Restore Point (prior to patch install) will reverse install of the Security Patch Update if recovery is required and is much faster than the full FreeFlow® Print Server System Restore. We recommend performing a full FreeFlow® Print Server System Backup for redundancy purposes in case the checkpoint restore does not work. The only option for FreeFlow® Print Server system recovery may be the FreeFlow® Print Server System Backup if the system should become inoperable such that Windows® is not stable. Make sure to store the FreeFlow® Print Server System backup onto a remote storage location or USB/DVD media.

4.0 Disclaimer

The information provided in this Xerox Product Response is provided "as is" without 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.

© 2026 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design®, FreeFlow®, and Brenva™, Baltoro™ and iGen®, are trademarks of Xerox Corporation in the United States and/or other countries.BR21127



Other company trademarks are also acknowledged.