Xerox Security Bulletin XRX25-015

Xerox® FreeFlow® Print Server v2 / Windows® 10

Install Method: USB/DVD Media

Supports:

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

Deliverable: July 2025 Security Patch Update
Includes: OpenJDK Java 8 Update 462-b09, Apache HTTP 2.4.64, Apache Tomcat 6.0.45, OpenSSL 3.5.1, OpenSSH 10.0p2 and Firefox 140.0.4 Software
Bulletin Date: August 13, 2025

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. **July 2025 Security Patch Update**
   - This supersedes the April 2025 Security Patch Update.
2. **OpenJDK Java 8 Update 462-b09 Software**
   - This supersedes OpenJDK Java 8 Update 452-b08 Software.
3. **Firefox 140.0.4 Software**
   - This supersedes Firefox 137.0.2 Software.
4. **Apache HTTP 2.4.64 Software**
   - This supersedes Apache HTTP 2.4.63 Software.
5. **Apache Tomcat 6.0.45 Software**
   - Same as delivered with previous April 2025 Security Patch Update.
6. **OpenSSL 3.5.1 Software**
   - This supersedes OpenSSL.3.4.0 Software.
7. **Open SSH 10.0p2**
   - This supersedes Open SSH 9.9p1 Software.

Although these July version patches were tested with the above FFPS v24 software release, there should be no problem installing the July 2025 Security Patch Update on earlier software releases.

Notice: The July 2025 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.).

See US-CERT Common Vulnerability Exposures (CVE) for the July 2025 Security Patch Update in table below:

July 2025 Security Patch Update Remediated US-CERT CVE's					
CVE-2024-36350	CVE-2025-47984	CVE-2025-48803	CVE-2025-48819	CVE-2025-49667	CVE-2025-49721
CVE-2024-36357	CVE-2025-47985	CVE-2025-48804	CVE-2025-48820	CVE-2025-49675	CVE-2025-49722
CVE-2025-47159	CVE-2025-47986	CVE-2025-48805	CVE-2025-48821	CVE-2025-49678	CVE-2025-49725
CVE-2025-47971	CVE-2025-47987	CVE-2025-48806	CVE-2025-48822	CVE-2025-49679	CVE-2025-49726
CVE-2025-47972	CVE-2025-47991	CVE-2025-48808	CVE-2025-48823	CVE-2025-49680	CVE-2025-49727
CVE-2025-47973	CVE-2025-47996	CVE-2025-48811	CVE-2025-49658	CVE-2025-49683	CVE-2025-49730
CVE-2025-47975	CVE-2025-47999	CVE-2025-48814	CVE-2025-49659	CVE-2025-49684	CVE-2025-49732
CVE-2025-47976	CVE-2025-48000	CVE-2025-48815	CVE-2025-49660	CVE-2025-49686	CVE-2025-49740
CVE-2025-47980	CVE-2025-48001	CVE-2025-48816	CVE-2025-49661	CVE-2025-49687	CVE-2025-49742
CVE-2025-47981	CVE-2025-48799	CVE-2025-48817	CVE-2025-49664	CVE-2025-49689	CVE-2025-49744
CVE-2025-47982	CVE-2025-48800	CVE-2025-48818	CVE-2025-49665	CVE-2025-49691	CVE-2025-49760

Note: The official Microsoft® patches included in the July 2025 Security Patch Update are KB5062560, KB5062799 and KB890830.

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 462-b09 software below:

OpenJDK 8 Update 462-b09 Software Remediated US-CERT CVE's					
CVE-2025-30749	CVE-2025-30754	CVE-2025-30761	CVE-2025-50106		

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache HTTP 2.4.64 software below:

Apache HTTP 2.4.64 Remediated US-CERT CVE's			
CVE-2025-53020	CVE-2025-49630	CVE-2024-47252	CVE-2024-43204
CVE-2025-49812	CVE-2025-23048	CVE-2024-43394	CVE-2024-42516

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenSSL 3.5.1software below:

OpenSSL 3.5.1Software Remediated US-CERT CVE's				
CVE-2024-12797	CVE-2024-13176	CVE-2025-4575		

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox 140.0.4 software below:

Firefox 140.0.4 Software Remediated US-CERT CVE's					
CVE-2025-2817	CVE-2025-4089	CVE-2025-5264	CVE-2025-5272	CVE-2025-6429	CVE-2025-6436
CVE-2025-4082	CVE-2025-4090	CVE-2025-5265	CVE-2025-5283	CVE-2025-6430	CVE-2025-49709
CVE-2025-4083	CVE-2025-4091	CVE-2025-5266	CVE-2025-6424	CVE-2025-6431	CVE-2025-49710
CVE-2025-4085	CVE-2025-4092	CVE-2025-5267	CVE-2025-6425	CVE-2025-6432	
CVE-2025-4086	CVE-2025-4918	CVE-2025-5268	CVE-2025-6426	CVE-2025-6433	
CVE-2025-4087	CVE-2025-4919	CVE-2025-5270	CVE-2025-6427	CVE-2025-6434	
CVE-2025-4088	CVE-2025-5263	CVE-2025-5271	CVE-2025-6428	CVE-2025-6435	

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 July 2025 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 July 2025 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
Brenva™ HD Inkjet	CP.24.0.22200.0 / CP.24.0.23126.0

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_Apr2025.zip	2,250,735	2,304,751,813
FFPSv2-Win10_SecPatchUpdate_Apr2025.iso	2,251,086	2,305,112,064

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.