Xerox Security Bulletin XRX25-009

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: April 2025 Security Patch Update
Includes: OpenJDK Java 8 Update 452-b08, Apache HTTP 2.4.63, Apache Tomcat 6.0.45, OpenSSL 3.4.0, OpenSSH 9.9p1 and Firefox 137.0.2 Software
Bulletin Date: May 12, 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. **April 2025 Security Patch Update**
   - This supersedes the January 2025 Security Patch Update.
2. **OpenJDK Java 8 Update 452-b08 Software**
   - This supersedes OpenJDK Java 8 Update 442-b06 Software.
3. **Firefox 137.0.2 Software**
   - This supersedes Firefox 134.0.1 Software.
4. **Apache HTTP 2.4.63 Software**
   - Same as delivered with previous January 2025 Security Patch Update.
5. **Apache Tomcat 6.0.45 Software**
   - Same as delivered with previous January 2025 Security Patch Update.
6. **OpenSSL 3.4.0 Software**
   - Same as delivered with previous January 2025 Security Patch Update.
7. **Open SSH 9.9p1**
   - Same as delivered with previous January 2025 Security Patch Update.

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

Notice: The April 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 April 2025 Security Patch Update in table below:

April 2025 Security Patch Update Remediated US-CERT CVE's					
CVE-2025-21191	CVE-2025-26641	CVE-2025-26673	CVE-2025-27477	CVE-2025-27732	CVE-2025-29809
CVE-2025-21197	CVE-2025-26648	CVE-2025-26679	CVE-2025-27478	CVE-2025-27733	CVE-2025-29810
CVE-2025-21204	CVE-2025-26663	CVE-2025-26686	CVE-2025-27481	CVE-2025-27735	CVE-2025-29824
CVE-2025-21205	CVE-2025-26665	CVE-2025-26687	CVE-2025-27483	CVE-2025-27736	
CVE-2025-21221	CVE-2025-26668	CVE-2025-26688	CVE-2025-27484	CVE-2025-27737	
CVE-2025-21222	CVE-2025-26669	CVE-2025-27469	CVE-2025-27487	CVE-2025-27738	
CVE-2025-24073	CVE-2025-26670	CVE-2025-27471	CVE-2025-27491	CVE-2025-27741	
CVE-2025-26637	CVE-2025-26672	CVE-2025-27473	CVE-2025-27727	CVE-2025-27742	

Note: The official Oracle® patches included in the April 2025 Security Patch Update are KB5055521, KB5055661 and KB890830.

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 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 the Firefox 137.0.2 software below:

Firefox 137.0.2 Software Remediated US-CERT CVE's					
CVE-2025-3608					

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

Apache HTTP 2.4.63 Software Remediated US-CERT CVE's					
N/A					

Note: There are no CVE mitigations included in this Apache HTTP update. It only includes bug fixes.

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenSSL 3.4.0 software below:

OpenSSL 3.4.0 Software Remediated US-CERT CVE's				
CVE-2024-9143	CVE-2024-12797	CVE-2024-13176		

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 April 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 April 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
Baltoro™ HF Inkjet	CP.24.0.23126.0
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	2,224,581	2,277,970,119
FFPSv2-Win10_SecPatchUpdate_Apr2025.iso	2,224,932	2,278,330,368

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.