Xerox Security Bulletin XRX23-021

Xerox® FreeFlow® Print Server v2 / Windows® 10

Install Method: Hard Disk / USB Media

Supports:

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

Deliverable: October 2023 Security Patch Update
Includes: OpenJDK Java 8 Update 392-b07, Apache 2.4.58 and Firefox 119.0 Software
Bulletin Date: November 27, 2023

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 (i.e., 4 times a year) 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.

Notice: This patch update includes mitigation for the PrintNightmare vulnerability which resides in the Windows Print Spooler service and affects the Windows Print Queue. The PrintNightmare vulnerability enables attackers to execute remote code on our devices, and thus take control over them.

This bulletin announces the availability of the following:

1. **October 2023 Security Patch Update**
   - This supersedes the July 2023 Security Patch Update
2. **OpenJDK Java 8 Update 392-b07 Software**
   - This supersedes OpenJDK Java 8 Update 382-b09 Software.
3. **Firefox v119.0 Software**
   - This supersedes Firefox v115.0.3
4. **Apache v2.4.58 Software**
   - This supersedes Apache v2.4.57

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache v2.4.58 software below:

Apache v2.4.58 Software Remediated US-CERT CVE's			
CVE-2023-31122	CVE-2023-43622	CVE-2023-45802	

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 392-b07 software below:

OpenJDK Java 8 Update 392-b07 Software Remediated US-CERT CVE's			
CVE-2023-22025	CVE-2023-22067	CVE-2023-22081	

See US-CERT Common Vulnerability Exposures (CVE) for the October 2023 Security Patch Update in table below:

October 2023 Security Patch Update Remediated US-CERT CVE's					
CVE-2023-35349	CVE-2023-36572	CVE-2023-36584	CVE-2023-36606	CVE-2023-36720	CVE-2023-38166
CVE-2023-36431	CVE-2023-36573	CVE-2023-36585	CVE-2023-36697	CVE-2023-36722	CVE-2023-41765
CVE-2023-36434	CVE-2023-36574	CVE-2023-36589	CVE-2023-36701	CVE-2023-36724	CVE-2023-41766
CVE-2023-36436	CVE-2023-36575	CVE-2023-36590	CVE-2023-36702	CVE-2023-36726	CVE-2023-41767
CVE-2023-36438	CVE-2023-36576	CVE-2023-36591	CVE-2023-36709	CVE-2023-36729	CVE-2023-41768
CVE-2023-36557	CVE-2023-36577	CVE-2023-36592	CVE-2023-36710	CVE-2023-36731	CVE-2023-41769
CVE-2023-36563	CVE-2023-36578	CVE-2023-36593	CVE-2023-36711	CVE-2023-36732	CVE-2023-41770
CVE-2023-36564	CVE-2023-36579	CVE-2023-36594	CVE-2023-36712	CVE-2023-36743	CVE-2023-41771
CVE-2023-36567	CVE-2023-36581	CVE-2023-36596	CVE-2023-36713	CVE-2023-36776	CVE-2023-41773
CVE-2023-36570	CVE-2023-36582	CVE-2023-36598	CVE-2023-36717	CVE-2023-36902	CVE-2023-41774
CVE-2023-36571	CVE-2023-36583	CVE-2023-36602	CVE-2023-36718	CVE-2023-38159	CVE-2023-44487

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v119.0 software below:

Firefox v119.0 Software Remediated US-CERT CVE's					
CVE-2023-4045	CVE-2023-4054	CVE-2023-4577	CVE-2023-4863	CVE-2023-5176	CVE-2023-5727
CVE-2023-4046	CVE-2023-4055	CVE-2023-4578	CVE-2023-5168	CVE-2023-5217	CVE-2023-5728
CVE-2023-4047	CVE-2023-4056	CVE-2023-4579	CVE-2023-5169	CVE-2023-5721	CVE-2023-5729
CVE-2023-4048	CVE-2023-4057	CVE-2023-4580	CVE-2023-5170	CVE-2023-5722	CVE-2023-5730
CVE-2023-4049	CVE-2023-4058	CVE-2023-4581	CVE-2023-5171	CVE-2023-5722	CVE-2023-5731
CVE-2023-4050	CVE-2023-4573	CVE-2023-4582	CVE-2023-5172	CVE-2023-5723	CVE-2023-5732
CVE-2023-4051	CVE-2023-4574	CVE-2023-4583	CVE-2023-5173	CVE-2023-5724	
CVE-2023-4052	CVE-2023-4575	CVE-2023-4584	CVE-2023-5174	CVE-2023-5725	
CVE-2023-4053	CVE-2023-4576	CVE-2023-4585	CVE-2023-5175	CVE-2023-5726	

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 October 2023 Security Patch Update (including OpenJDK Java 8 Update 392-b07 software, and Firefox v115.0.3Patches) is available for the FreeFlow® Print Server v2 Software Release running on Windows® v10 OS. The FreeFlow® Print Server software release tested with the October 2023 Security Patch Update installed per printer products is illustrated below:

Printer Products	Patch Update Tested Releases
iGen®5 Press	CP.24.0.22200.0
Baltoro™ HF Inkjet	CP.24.0.22200.0 / CP.24.0.23126.0
Brenva™ HD Inkjet	CP.24.0.22200.0

Although these October version patches were tested with the above FFPS v24 software release, there should be no problem installing the October 2023 Security Patch Update 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 install 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).

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 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 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 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_Oct2023.zip	2,146,566	2,198,082,956
FFPSv2-Win10_SecPatchUpdate_Oct2023.iso	2,146,916	2,198,441,984

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 checking for the Windows® patch updates and installing them. This will give assurance of 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 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.