

Xerox Security Bulletin XRX23-002

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: January 2023 Security Patch Update

Includes: OpenJDK Java 8 Update 362-b09 Software

Bulletin Date: March 8, 20223

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. **January 2023 Security Patch Update**
 - This supersedes the October 2022 Security Patch Update
2. **OpenJDK Java 8 Update 362-b09 Software**
 - This supersedes OpenJDK Java 8 Update 342-b07 Software.
3. **Firefox v110.0 Software**
 - This supersedes Firefox v106.0.5
4. **Apache v2.4.55 Software**

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 362-b09 software below:

OpenJDK Java 8 Update 362-b09 Software Remediated US-CERT CVE's			
CVE-2023-21830	CVE-2023-21835	CVE-2023-21843	

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache v2.4.55 software below:

Apache v2.4.55 Software Remediated US-CERT CVE's			
CVE-2006-20001	CVE-2022-36760	CVE-2022-37436	

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

January 2023 Security Patch Update Remediated US-CERT CVE's					
CVE-2023-21684	CVE-2023-21691	CVE-2023-21699	CVE-2023-21799	CVE-2023-21812	CVE-2023-21822
CVE-2023-21685	CVE-2023-21692	CVE-2023-21700	CVE-2023-21801	CVE-2023-21813	CVE-2023-21823
CVE-2023-21686	CVE-2023-21693	CVE-2023-21701	CVE-2023-21802	CVE-2023-21816	CVE-2023-23376
CVE-2023-21688	CVE-2023-21694	CVE-2023-21702	CVE-2023-21804	CVE-2023-21817	
CVE-2023-21689	CVE-2023-21695	CVE-2023-21797	CVE-2023-21805	CVE-2023-21818	
CVE-2023-21690	CVE-2023-21697	CVE-2023-21798	CVE-2023-21811	CVE-2023-21820	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v110.0 software below:

Firefox v110.0 Software Remediated US-CERT CVE's					
CVE-2023-0767	CVE-2022-45411	CVE-2022-46871	CVE-2023-23597	CVE-2023-25728	CVE-2023-25738
CVE-2022-40674	CVE-2022-45412	CVE-2022-46872	CVE-2023-23598	CVE-2023-25729	CVE-2023-25739
CVE-2022-45403	CVE-2022-45413	CVE-2022-46873	CVE-2023-23599	CVE-2023-25730	CVE-2023-25740
CVE-2022-45404	CVE-2022-45415	CVE-2022-46874	CVE-2023-23600	CVE-2023-25731	CVE-2023-25741
CVE-2022-45405	CVE-2022-45416	CVE-2022-46875	CVE-2023-23601	CVE-2023-25732	CVE-2023-25742
CVE-2022-45406	CVE-2022-45417	CVE-2022-46877	CVE-2023-23602	CVE-2023-25733	CVE-2023-25743
CVE-2022-45407	CVE-2022-45418	CVE-2022-46878	CVE-2023-23603	CVE-2023-25734	CVE-2023-25744
CVE-2022-45408	CVE-2022-45419	CVE-2022-46879	CVE-2023-23604	CVE-2023-25735	CVE-2023-25745
CVE-2022-45409	CVE-2022-45420	CVE-2022-46882	CVE-2023-23605	CVE-2023-25736	
CVE-2022-45410	CVE-2022-45421	CVE-2022-46883	CVE-2023-23606	CVE-2023-25737	

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 2023 Security Patch Update (including OpenJDK Java 8 Update 362-b09 software, and Firefox v110.0 Patches) is available for the FreeFlow® Print Server v2 Software Release running on Windows® v10 OS. The FreeFlow® Print Server software releases tested with the January 2023 Security Patch Update installed per printer products is illustrated below:

Printer Products	Patch Update Tested Releases
iGen®5 Press	CP.24.19298.1 CP.24.21335.1
Baltoro™ HF Inkjet	CP.24.20111.1 CP.24.21335.1
Brenva™ HD Inkjet	CP.24.19114.0 CP.24.21335.1

All of the listed printer products were tested with each of the releases listed.

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_Jan2023.zip	4,224,997	4,326,396,268

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.