Xerox Security Bulletin XRX24-013

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: July 2024 Security Patch Update
Includes: OpenJDK Java 8 Update 422-b05, Apache 2.4.62, OpenSSL 3.1.6 and Firefox 128.0 Software
Bulletin Date: September 4, 2024

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 9he 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 2024 Security Patch Update**
   - This supersedes the April 2024 Security Patch Update
2. **OpenJDK Java 8 Update 422-b05 Software**
   - This supersedes OpenJDK Java 8 Update 412-b08 Software.
3. **Firefox 128.0 Software**
   - This supersedes Firefox 125.0.3 Software.
4. **Apache 2.4.62 Software**
   - Supersedes Apache 2.4.59 Software.
5. **OpenSSL 3.1.6 Software**
   - Supersedes OpenSSL 3.1.5 Software.

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache 2.4.62 software below:

Apache 2.4.62 Software Remediated US-CERT CVE's					
CVE-2024-36387	CVE-2024-38473	CVE-2024-38475	CVE-2024-38477	CVE-2024-39884	CVE-2024-40898
CVE-2024-38472	CVE-2024-38474	CVE-2024-38476	CVE-2024-39573	CVE-2024-40725	

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenSSL 3.1.6 software below:

OpenSSL 3.1.6 Software Remediated US-CERT CVE's				
CVE-2024-2511	CVE-2024-4603	CVE-2024-4741		

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 422-b05 software below:

OpenJDK 8 Update 422-b05 Software Remediated US-CERT CVE's					
CVE-2024-21131	CVE-2024-21138	CVE-2024-21140	CVE-2024-21144	CVE-2024-21145	CVE-2024-21147

See US-CERT Common Vulnerability Exposures (CVE) for the July 2024 Security Patch Update in table below:

July 2024 Security Patch Update Remediated US-CERT CVE's					
CVE-2024-28899	CVE-2024-37972	CVE-2024-38013	CVE-2024-38043	CVE-2024-38057	CVE-2024-38079
CVE-2024-30013	CVE-2024-37973	CVE-2024-38017	CVE-2024-38047	CVE-2024-38058	CVE-2024-38085
CVE-2024-30071	CVE-2024-37974	CVE-2024-38019	CVE-2024-38048	CVE-2024-38060	CVE-2024-38091
CVE-2024-30079	CVE-2024-37975	CVE-2024-38022	CVE-2024-38049	CVE-2024-38061	CVE-2024-38101
CVE-2024-30081	CVE-2024-37984	CVE-2024-38025	CVE-2024-38050	CVE-2024-38062	CVE-2024-38102
CVE-2024-30098	CVE-2024-37986	CVE-2024-38027	CVE-2024-38051	CVE-2024-38064	CVE-2024-38104
CVE-2024-35270	CVE-2024-37987	CVE-2024-38028	CVE-2024-38052	CVE-2024-38065	CVE-2024-38105
CVE-2024-3596	CVE-2024-37988	CVE-2024-38030	CVE-2024-38053	CVE-2024-38066	CVE-2024-38112
CVE-2024-37969	CVE-2024-37989	CVE-2024-38033	CVE-2024-38054	CVE-2024-38068	CVE-2024-38517
CVE-2024-37970	CVE-2024-38010	CVE-2024-38034	CVE-2024-38055	CVE-2024-38069	CVE-2024-39684
CVE-2024-37971	CVE-2024-38011	CVE-2024-38041	CVE-2024-38056	CVE-2024-38070	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox 128.0 software below:

Firefox 128.0 Software Remediated US-CERT CVE's					
CVE-2024-4367	CVE-2024-4771	CVE-2024-5687	CVE-2024-5695	CVE-2024-6601	CVE-2024-6609
CVE-2024-4771	CVE-2024-4772	CVE-2024-5688	CVE-2024-5696	CVE-2024-6602	CVE-2024-6610
CVE-2024-4772	CVE-2024-4773	CVE-2024-5689	CVE-2024-5697	CVE-2024-6603	CVE-2024-6611
CVE-2024-4773	CVE-2024-4774	CVE-2024-5690	CVE-2024-5698	CVE-2024-6604	CVE-2024-6612
CVE-2024-4774	CVE-2024-4775	CVE-2024-5691	CVE-2024-5699	CVE-2024-6605	CVE-2024-6613
CVE-2024-4775	CVE-2024-4776	CVE-2024-5692	CVE-2024-5700	CVE-2024-6606	CVE-2024-6614
CVE-2024-4776	CVE-2024-4777	CVE-2024-5693	CVE-2024-5701	CVE-2024-6607	CVE-2024-6615
CVE-2024-4777	CVE-2024-4778	CVE-2024-5694	CVE-2024-6600	CVE-2024-6608	
CVE-2024-4778	CVE-2024-4771	CVE-2024-5687	CVE-2024-5695	CVE-2024-6601	

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 2024 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 2024 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

Although these July 2024 version patches were tested with the above FFPS v24 software release, there should be no problem installing the July 2024 Security Patch Update on earlier software releases.

Notice: The Security Patch Cluster created 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.).

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).

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_Jul2024.zip	2,214,672	2,267,823,290
FFPSv2-Win10_SecPatchUpdate_Jul2024.iso	2,215,022	2,268,182,528

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.