Xerox Security Bulletin XRX24-011

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: April 2024 Security Patch Update
Includes: OpenJDK Java 8 Update 412-b08, Apache HTTP 2.4.59, Apache Tomcat 6.0.45, OpenSSL 3.1.5 and Firefox 125.0.3 Software
Bulletin Date: May 29, 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 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 2024 Security Patch Update**
   - This supersedes the January 2024 Security Patch Update
2. **OpenJDK Java 8 Update 412-b08 Software**
   - This supersedes OpenJDK Java 8 Update 402-b09 Software.
3. **Firefox 125.0.3 Software**
   - This supersedes Firefox 121.0.1 Software.
4. **Apache HTTP 6.0.45 Software**
   - Supersedes Apache HTTP 2.4.58 Software.
5. **Apache Tomcat 2.4.59 Software**
6. **OpenSSL 3.1.5 Software**
   - Supersedes OpenSSL 3.1.3 Software.

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

Notice: The April 2024 Security Patch Cluster creates some noteworthy issues. The caveats after installing these Security patches are as follows:

1. There is a Brenva Inkjet printer prerequisite to first ensure the January 2024 Security Patch Cluster is installed prior to installing the April 2024 Security Patch Cluster. The April 2024 Security Patch Cluster will not install correctly for Brenva if the January 2024 Security Patch Cluster is not installed first.

2. 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.

   The Xear Flex application is no longer able to connect to the printer using a secure FTP (SFTP) request until updated with stronger encryption algorithms. A customer may refuse to install the April 2024 Security Patch Cluster if it breaks their secure connection for Xear Flex until there is a fix for this issue. A customer would need to determine if Xear Flex or installing the latest Security Patch Cluster is more important to them.

3. 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 2024 Security Patch Update in table below:

April 2024 Security Patch Update Remediated US-CERT CVE's					
CVE-2022-0001	CVE-2024-26168	CVE-2024-26211	CVE-2024-26240	CVE-2024-28898	CVE-2024-28925
CVE-2024-20693	CVE-2024-26171	CVE-2024-26214	CVE-2024-26241	CVE-2024-28900	CVE-2024-29050
CVE-2024-20665	CVE-2024-26175	CVE-2024-26217	CVE-2024-26242	CVE-2024-28901	CVE-2024-29061
CVE-2024-20669	CVE-2024-26179	CVE-2024-26220	CVE-2024-26244	CVE-2024-28902	CVE-2024-29062
CVE-2024-20678	CVE-2024-26180	CVE-2024-26228	CVE-2024-26248	CVE-2024-28903	CVE-2024-29064
CVE-2024-26207	CVE-2024-26183	CVE-2024-26229	CVE-2024-26250	CVE-2024-28919	
CVE-2024-26208	CVE-2024-26189	CVE-2024-26230	CVE-2024-26252	CVE-2024-28921	
CVE-2024-26209	CVE-2024-26194	CVE-2024-26232	CVE-2024-26253	CVE-2024-28922	
CVE-2024-26210	CVE-2024-26200	CVE-2024-26234	CVE-2024-28896	CVE-2024-28923	
CVE-2024-26158	CVE-2024-26205	CVE-2024-26239	CVE-2024-28897	CVE-2024-28924	

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 412-b08 software below:

OpenJDK 8 Update 412-b08 Software Remediated US-CERT CVE's					
CVE-2024-21011	CVE-2024-21068	CVE-2024-21085	CVE-2024-21094		

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache HTTP 2.4.59 software below:

Apache HTTP 2.4.59 Software Remediated US-CERT CVE's			
CVE-2024-24795	CVE-2024-27316	CVE-2023-38709	

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache Tomcat 6.0.45 software below:

Apache HTTP 2.4.59 Software Remediated US-CERT CVE's			
CVE-2024-24795	CVE-2024-27316	CVE-2023-38709	

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenSSL 3.1.5 software below:

OpenSSL 3.1.5 Software Remediated US-CERT CVE's				
CVE-2023-5363	CVE-2023-5678	CVE-2023-6129	CVE-2023-6237	CVE-2024-0727

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox 125.0.3 software below:

Firefox 125.0.3 Software Remediated US-CERT CVE's					
CVE-2024-0741	CVE-2024-0751	CVE-2024-1551	CVE-2024-2608	CVE-2024-3854	CVE-2024-3864
CVE-2024-0742	CVE-2024-0752	CVE-2024-1552	CVE-2024-2609	CVE-2024-3855	CVE-2024-3865
CVE-2024-0743	CVE-2024-0753	CVE-2024-1553	CVE-2024-2610	CVE-2024-3856	CVE-2024-3302
CVE-2024-0744	CVE-2024-0754	CVE-2024-1554	CVE-2024-2611	CVE-2024-3857	CVE-2023-5388
CVE-2024-0745	CVE-2024-0755	CVE-2024-1555	CVE-2024-2612	CVE-2024-3858	CVE-2024-29943
CVE-2024-0746	CVE-2024-1546	CVE-2024-1556	CVE-2024-2613	CVE-2024-3859	CVE-2024-29944
CVE-2024-0747	CVE-2024-1547	CVE-2024-1557	CVE-2024-2614	CVE-2024-3860	
CVE-2024-0748	CVE-2024-1548	CVE-2024-2605	CVE-2024-2615	CVE-2024-3861	
CVE-2024-0749	CVE-2024-1549	CVE-2024-2606	CVE-2024-3852	CVE-2024-3862	
CVE-2024-0750	CVE-2024-1550	CVE-2024-2607	CVE-2024-3853	CVE-2024-3863	

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 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 April 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

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_Apr2024.zip	2,182,675	2,235,058,810
FFPSv2-Win10_SecPatchUpdate_Apr2024.iso	2,183,026	2,235,418,624

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 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.