Xerox Security Bulletin XRX20-012

Xerox® FreeFlow® Print Server v2 / Windows® 10

Supports:

- Xerox® iGen®5 Press
- Xerox® BaltoroTM HF Production Inkjet Press
- Xerox® BrenvaTM HD Production Inkjet Press

Deliverable: April 2020 Security Patch Update
Includes: Java 8 Update 251
Bulletin Date: June 18, 2020

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.

This bulletin announces the availability of the following:

1. **April 2020 Security Patch Update**
   - This supersedes the January 2020 Security Patch Cluster
2. **Java 8 Update 251 Software**
   - This supersedes Java 8 Update 241 Software
3. **Firefox v75.0 Software**
   - This supersedes Firefox v72.0.2

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 8 Update 251 software below:

Java 8 Update 251 Software Remediated US-CERT CVE's				
CVE-2020-2754	CVE-2020-2757	CVE-2020-2778	CVE-2020-2803	CVE-2020-2830
CVE-2020-2755	CVE-2020-2764	CVE-2020-2781	CVE-2020-2805	CVE-2019-18197
CVE-2020-2756	CVE-2020-2773	CVE-2020-2800	CVE-2020-2816	

See US-CERT Common Vulnerability Exposures (CVE) for the April 2020 Security Patch Update in table below:

April 2020 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2020-0687	CVE-2020-0917	CVE-2020-0947	CVE-2020-0964	CVE-2020-0992	CVE-2020-1008
CVE-2020-0687	CVE-2020-0918	CVE-2020-0948	CVE-2020-0965	CVE-2020-0993	CVE-2020-1009
CVE-2020-0699	CVE-2020-0929	CVE-2020-0949	CVE-2020-0966	CVE-2020-0994	CVE-2020-1011
CVE-2020-0784	CVE-2020-0934	CVE-2020-0950	CVE-2020-0967	CVE-2020-0995	CVE-2020-1014
CVE-2020-0784	CVE-2020-0936	CVE-2020-0952	CVE-2020-0968	CVE-2020-0996	CVE-2020-1015
CVE-2020-0794	CVE-2020-0937	CVE-2020-0953	CVE-2020-0969	CVE-2020-0999	CVE-2020-1016
CVE-2020-0821	CVE-2020-0938	CVE-2020-0955	CVE-2020-0970	CVE-2020-1000	CVE-2020-1017
CVE-2020-0888	CVE-2020-0939	CVE-2020-0956	CVE-2020-0981	CVE-2020-1001	CVE-2020-1020
CVE-2020-0889	CVE-2020-0940	CVE-2020-0957	CVE-2020-0982	CVE-2020-1003	CVE-2020-1027
CVE-2020-0895	CVE-2020-0942	CVE-2020-0958	CVE-2020-0983	CVE-2020-1004	CVE-2020-1029
CVE-2020-0907	CVE-2020-0944	CVE-2020-0959	CVE-2020-0985	CVE-2020-1005	CVE-2020-1094
CVE-2020-0910	CVE-2020-0945	CVE-2020-0960	CVE-2020-0987	CVE-2020-1006	CVE-2020-3757
CVE-2020-0913	CVE-2020-0946	CVE-2020-0962	CVE-2020-0988	CVE-2020-1007	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v75.0 software below:

Firefox v75.0 Software Remediated US-CERT CVE's			
CVE-2019-20503	CVE-2020-6805	CVE-2020-6812	CVE-2020-6822
CVE-2020-6796	CVE-2020-6806	CVE-2020-6813	CVE-2020-6823
CVE-2020-6797	CVE-2020-6807	CVE-2020-6814	CVE-2020-6824
CVE-2020-6798	CVE-2020-6808	CVE-2020-6815	CVE-2020-6825
CVE-2020-6799	CVE-2020-6809	CVE-2020-6819	CVE-2020-6826
CVE-2020-6800	CVE-2020-6810	CVE-2020-6820	
CVE-2020-6801	CVE-2020-6811	CVE-2020-6821	

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 tested by Xerox.

2.0 Applicability

This April 2020 Security Patch Update (including Java 8 Update 251 software, and Firefox v75.0 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 April 2020 Security Patch Update installed per printer products is illustrated below:

Printer Producs	Patch Update Tested Releases
iGen®5 Press Baltoro™ HF Inkjet Brenva™ HD Inkjet	CP.24.0.18201.0
	CP.24.0.19114.0
	CP.24.0.19119.0

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

2.1 Available Patch Update Install Methods

Xerox offers the Security Patch Update delivery available over the network from a Xerox server using an application called FreeFlow® Print Server Update Manager. The use of Update Manager (GUI-based application) makes it simple for a customer to install Security patch updates. Downloading and installing Security Patch Updates using the Update Manager has the advantage of "ease of use" as it involves accessing the Security Patch Update from a Xerox Server over the network.

In addition, the FreeFlow® Print Server Security Patch Update is available for a delivery method using media (USB) for the install. The FreeFlow® Print Server customer schedules a Xerox Analyst or Service Engineer (CSE) to install the Security Patch Update at the customer account. The Analyst/CSE can choose to work with a customer and allow them to install the Security Patch Updates from USB media.

A customer can also manage Security Patch Updates from a Microsoft® server on their own using Windows® Update service built into the Operating System. This is a GUI-based application used to schedule automatic patch updates, or to perform manual updates selecting a '**Check for Updates**' option. This method has the advantage of retrieving Security patches at the soonest time possible. It also has most risk given the install of these Security patches directly from Microsoft® untested on the FreeFlow® Print Server platform by Xerox.

2.2 Security Considerations

Security of the network, devices and information on a customer network may be a consideration when deciding whether to use the USB, FreeFlow® Print Server Update Manager or Windows® Update method of Security Patch Update delivery and install. When using Update Manager, the external Xerox server that includes the Security Patch Update does not have access to the FreeFlow® Print Server platform at a customer site.

The FreeFlow® Print Server platform (using Update Manager) initiates all communication to download the FreeFlow® Print Server Security Patch Update, and the communication is "secure" by TLS 1.0 over HTTPS (port 443) with the Xerox communication server. This communication uses an RSA 2048-bit certificate, SHA2 hash and AES 256-bit stream encryption algorithms. This connection ensures authentication of the FreeFlow® Print Server platform for the Xerox server, and sets up encrypted communication of the patch data. The Xerox server does not initiate or have access to the FreeFlow® Print Server platform behind the customer firewall. The Xerox server and FreeFlow® Print Server system both authenticate each other before making a connection between the two endpoints, and patch data transfer.

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 Update Manager Delivery

The Update Manager is a GUI tool on the FreeFlow® Print Server platform used to check for Security updates, download Security updates, and install Security updates. The customer can install quarterly FreeFlow® Print Server Security Patch Updates using the Update Manager UI, or schedule Xerox Service to perform the install.

Once the Security patches are ready for customer delivery, they are available from the Xerox Edge Host and Download servers. Procedures are available for the FreeFlow® Print Server System Administrator or Xerox Service for using the Update Manager GUI to download and install the Security patches over the Internet. The Update Manager UI has a '**Check for Updates**' button that can be selected to retrieve and list patch updates available from the Xerox patch server. When this option is selected the latest Security Patch Update should be listed (E.g., **April 2020 Security Patch Update for FFPS v2 / Windows 10**) as available for download and install. The Update Manager UI includes mouse selectable buttons to download and then install the patches.

Xerox uploads the FreeFlow® Print Server Security Patch Update to a Xerox patch server that is available on the Internet outside of the Xerox Corporate network once the deliverable has been tested and approved. Once in place on the Xerox server, a CSE/Analyst or the customer can use the Update Manager UI to download and install on the FreeFlow® Print Server platform.

The customer proxy information is required to be setup on the FreeFlow® Print Server platform so it can access to the Security Patch Update over the Internet. The FreeFlow® Print Server platform initiates a "secure" communication session with the Xerox patch server using HTTP over the TSL 1.0 protocol (HTTPS on port 443) using an RSA 2048-bit certificate, SHA2 hash and AES 256-bit stream encryption algorithms.

This connection ensures authentication of the FreeFlow® Print Server platform for the Xerox server, and sets up encrypted communication of the patch data. The Xerox server does not initiate or have access to the FreeFlow® Print Server platform behind the customer firewall. The Xerox server and FreeFlow® Print Server system both authenticate each other before making a connection between the two endpoints, and patch data transfer.

3.2 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® File Size (K-bytes)	Size in Bytes
FFPSv2-Win10_SecPatchUpdate_Apr2020.zip	3,223,065	3,300,417,649

3.3 Windows® Update Delivery

Windows® Update services enables 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.