Xerox Security Bulletin XRX21-004

Xerox® FreeFlow® Print Server v2 / Windows® 10

Install Method: USB Media

Supports:

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

Deliverable: January 2021 Security Patch Update
Includes: OpenJDK 1.8.0-102021
Bulletin Date: February 8, 2021

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. **January 2021 Security Patch Update**
   - This supersedes the October 2020 Security Patch Update
2. **Open JDK 1.8.0-012021Software**
   - This supersedes JDK 1.8.0-102020 Software
3. **Firefox v85.0 Software**
   - This supersedes Firefox v81.0.2

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 1.8.0-102021 software below:

OpenJDK 1.8.0-012021 Software Remediated US-CERT CVE's			
CVE-2020-14803			

See US-CERT Common Vulnerability Exposures (CVE) for the January 2021 Security Patch Update in table below:

January 2021 Security Patch Update Remediated US-CERT CVE's					
CVE-2020-0689	CVE-2021-1653	CVE-2021-1665	CVE-2021-1679	CVE-2021-1690	CVE-2021-1702
CVE-2020-0733	CVE-2021-1654	CVE-2021-1666	CVE-2021-1680	CVE-2021-1692	CVE-2021-1704
CVE-2021-1637	CVE-2021-1655	CVE-2021-1667	CVE-2021-1681	CVE-2021-1693	CVE-2021-1706
CVE-2021-1642	CVE-2021-1656	CVE-2021-1668	CVE-2021-1683	CVE-2021-1694	CVE-2021-1708
CVE-2021-1645	CVE-2021-1657	CVE-2021-1669	CVE-2021-1684	CVE-2021-1695	CVE-2021-1709
CVE-2021-1648	CVE-2021-1658	CVE-2021-1671	CVE-2021-1685	CVE-2021-1696	CVE-2021-1710
CVE-2021-1649	CVE-2021-1659	CVE-2021-1673	CVE-2021-1686	CVE-2021-1697	
CVE-2021-1650	CVE-2021-1660	CVE-2021-1674	CVE-2021-1687	CVE-2021-1699	
CVE-2021-1651	CVE-2021-1661	CVE-2021-1676	CVE-2021-1688	CVE-2021-1700	
CVE-2021-1652	CVE-2021-1664	CVE-2021-1678	CVE-2021-1689	CVE-2021-1701	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v 85.0 software below:

Firefox v85.0 Software Remediated US-CERT CVE's					
CVE-2020-15999	CVE-2020-26955	CVE-2020-26964	CVE-2020-26974	CVE-2020-35114	CVE-2021-23962
CVE-2020-16012	CVE-2020-26956	CVE-2020-26965	CVE-2020-26975	CVE-2021-23953	CVE-2021-23963
CVE-2020-16042	CVE-2020-26957	CVE-2020-26966	CVE-2020-26976	CVE-2021-23954	CVE-2021-23964
CVE-2020-16044	CVE-2020-26958	CVE-2020-26967	CVE-2020-26977	CVE-2021-23955	CVE-2021-23965
CVE-2020-26950	CVE-2020-26959	CVE-2020-26968	CVE-2020-26978	CVE-2021-23956	
CVE-2020-26951	CVE-2020-26960	CVE-2020-26969	CVE-2020-26979	CVE-2021-23957	
CVE-2020-26952	CVE-2020-26961	CVE-2020-26971	CVE-2020-35111	CVE-2021-23958	
CVE-2020-26953	CVE-2020-26962	CVE-2020-26972	CVE-2020-35112	CVE-2021-23959	
CVE-2020-26954	CVE-2020-26963	CVE-2020-26973	CVE-2020-35113	CVE-2021-23960	

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 2021 Security Patch Update (including OpenJDK 1.8.0-102021 software, and Firefox v85.0 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 2021 Security Patch Update installed per printer products is illustrated below:

Printer Products	Patch Update Tested Releases
iGen®5 Press Baltoro^{TM} HF Inkjet Brenva^{TM} 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.

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_Jan2021.zip	6,974,435	7,141,820,750

3.2 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.