Xerox Security Bulletin XRX22-001

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 2022 Security Patch Update
Includes: OpenJDK Java 8 update 322-b08 Software
Bulletin Date: January 28, 2022

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 January, 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 2022 Security Patch Update**
   - This supersedes the October 2021 Security Patch Update
2. **OpenJDK Java 8 Update 322-b08 Software**
   - This supersedes **OpenJDK Java 8 Update 312-b08Software**
3. **Firefox v96.0.2 Software**
   - This supersedes Firefox v93.0

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK Java 8 Update 322-b08 software below:

OpenJDK Java 8 Update 322-b08 Software Remediated US-CERT CVE's			
CVE-2022-21248	CVE-2022-21291	CVE-2022-21299	CVE-2022-21349
CVE-2022-21277	CVE-2022-21293	CVE-2022-21305	CVE-2022-21360
CVE-2022-21282	CVE-2022-21294	CVE-2022-21340	CVE-2022-21365
CVE-2022-21283	CVE-2022-21296	CVE-2022-21341	CVE-2022-21366

See US-CERT Common Vulnerability Exposures (CVE) for the January 2022 Security Patch Update in table below:

January 2022 Security Patch Update Remediated US-CERT CVE's					
CVE-2022-21833	CVE-2022-21857	CVE-2022-21873	CVE-2022-21889	CVE-2022-21903	CVE-2022-21922
CVE-2022-21834	CVE-2022-21860	CVE-2022-21874	CVE-2022-21890	CVE-2022-21904	CVE-2022-21924
CVE-2022-21835	CVE-2022-21862	CVE-2022-21875	CVE-2022-21892	CVE-2022-21905	CVE-2022-21928
CVE-2022-21836	CVE-2022-21863	CVE-2022-21876	CVE-2022-21893	CVE-2022-21908	CVE-2022-21958
CVE-2022-21838	CVE-2022-21864	CVE-2022-21878	CVE-2022-21894	CVE-2022-21913	CVE-2022-21959
CVE-2022-21843	CVE-2022-21866	CVE-2022-21879	CVE-2022-21895	CVE-2022-21914	CVE-2022-21960
CVE-2022-21848	CVE-2022-21867	CVE-2022-21880	CVE-2022-21897	CVE-2022-21915	CVE-2022-21961
CVE-2022-21849	CVE-2022-21868	CVE-2022-21881	CVE-2022-21900	CVE-2022-21916	CVE-2022-21962
CVE-2022-21850	CVE-2022-21870	CVE-2022-21883	CVE-2022-21901	CVE-2022-21919	CVE-2022-21964
CVE-2022-21851	CVE-2022-21871	CVE-2022-21885	CVE-2022-21902	CVE-2022-21920	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v96.0.2 software below:

Firefox v96.0.2 Software Remediated US-CERT CVE's					
CVE-2021-38503	CVE-2021-4128	CVE-2021-43536	CVE-2021-43544	CVE-2022-22741	CVE-2022-22749
CVE-2021-38504	CVE-2021-4129	CVE-2021-43537	CVE-2021-43545	CVE-2022-22742	CVE-2022-22750
CVE-2021-38505	CVE-2021-4140	CVE-2021-43538	CVE-2021-43546	CVE-2022-22743	CVE-2022-22751
CVE-2021-38506	CVE-2021-43530	CVE-2021-43539	CVE-2022-22736	CVE-2022-22744	CVE-2022-22752
CVE-2021-38507	CVE-2021-43531	CVE-2021-43540	CVE-2022-22737	CVE-2022-22745	
CVE-2021-38508	CVE-2021-43532	CVE-2021-43541	CVE-2022-22738	CVE-2022-22746	
CVE-2021-38509	CVE-2021-43533	CVE-2021-43542	CVE-2022-22739	CVE-2022-22747	
CVE-2021-38510	CVE-2021-43534	CVE-2021-43543	CVE-2022-22740	CVE-2022-22748	

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 2022 Security Patch Update (including OpenJDK Java 8 update 322-b08 software, and Firefox v96.0.2 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 2022 Security Patch Update installed per printer products is illustrated below:

Printer Products	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
	CP.24.0.20111.1

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_Jan2022.zip	2,492,742	2,552,567,649
FFPSv2-Win10_SecPatchUpdate_Jan2022.iso	2,493,092	2,552,926,208

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.