Xerox Security Bulletin XRX19-022

Xerox® FreeFlow® Print Server v2 (Windows 7)

Supports:

- Xerox® Color C60/C70 Printer
- Xerox® iGen®5 Press
- Xerox® Brenva™ HD Production InkJet Printer Products

Patch Version: July 2019 Security Patch Update
Includes: Java 8 Update 221, and Firefox v68.0.1 Patches
Bulletin Date: August 17, 2019

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® 7 and components (e.g., Windows® Explorer®, .Net Framework®, etc.). The FreeFlow® Print Server organization has a dedicated development team, which actively reviews 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® v7 (supporting the Integrated and Standalone platforms)

The FreeFlow® Print Server organization delivers Security Patch Updates on the FreeFlow® Print Server v2 / Windows® v7 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 July, July, July and October, and will test them for supported Printer products (listed in the document header) 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. **July 2019 Security Patch Update**
   - Supersedes the April 2019 Security Patch Update
2. **Java 8 Update 221 Software**
   - This supersedes Java 8 Update 211
3. **Firefox v68.0.1 Software**
   - This supersedes Firefox v66.0.3

See US-CERT Common Vulnerability Exposures (CVE) for the July 2019 Security Patch Update in table below:

July 2019 Security Patch Update Remediated US-CERT CVE's					
CVE-2019-0683	CVE-2019-0985	CVE-2019-1049	CVE-2019-1086	CVE-2019-1101	CVE-2019-1126
CVE-2019-0708	CVE-2019-0988	CVE-2019-1055	CVE-2019-1087	CVE-2019-1102	CVE-2019-1127
CVE-2019-0785	CVE-2019-0999	CVE-2019-1056	CVE-2019-1088	CVE-2019-1104	CVE-2019-1128
CVE-2019-0811	CVE-2019-1001	CVE-2019-1059	CVE-2019-1089	CVE-2019-1108	CVE-2019-1129
CVE-2019-0865	CVE-2019-1004	CVE-2019-1063	CVE-2019-1090	CVE-2019-1113	CVE-2019-1130
CVE-2019-0880	CVE-2019-1005	CVE-2019-1067	CVE-2019-1091	CVE-2019-1116	CVE-2019-1132
CVE-2019-0887	CVE-2019-1006	CVE-2019-1071	CVE-2019-1093	CVE-2019-1117	CVE-2019-11091
CVE-2019-0920	CVE-2019-1009	CVE-2019-1073	CVE-2019-1094	CVE-2019-1118	CVE-2018-12126
CVE-2019-0960	CVE-2019-1011	CVE-2019-1074	CVE-2019-1095	CVE-2019-1119	CVE-2018-12127
CVE-2019-0962	CVE-2019-1013	CVE-2019-1080	CVE-2019-1096	CVE-2019-1120	CVE-2018-12130
CVE-2019-0966	CVE-2019-1016	CVE-2019-1082	CVE-2019-1097	CVE-2019-1121	
CVE-2019-0968	CVE-2019-1037	CVE-2019-1083	CVE-2019-1098	CVE-2019-1122	
CVE-2019-0975	CVE-2019-1047	CVE-2019-1084	CVE-2019-1099	CVE-2019-1123	
CVE-2019-0977	CVE-2019-1048	CVE-2019-1085	CVE-2019-1100	CVE-2019-1124	

See the US-CERT Common Vulnerability Exposures (CVE) for the Java 8 Update 221 Software in table below:

Java 8 Update 221 Software Remediated US-CERT CVE's			
CVE-2019-7317	CVE-2019-2769	CVE-2019-2816	CVE-2019-2766
CVE-2019-2762	CVE-2019-2745	CVE-2019-2842	

See US-CERT Common Vulnerability Exposures (CVE) for the Firefox v68.0.1 Update in table below:

Firefox v68.0.1 Update Remediated US-CERT CVE's					
CVE-2019-7317	CVE-2019-9819	CVE-2019-11696	CVE-2019-11708	CVE-2019-11716	CVE-2019-11725
CVE-2019-9800	CVE-2019-9820	CVE-2019-11697	CVE-2019-11709	CVE-2019-11717	CVE-2019-11727
CVE-2019-9811	CVE-2019-9821	CVE-2019-11698	CVE-2019-11710	CVE-2019-11718	CVE-2019-11728
CVE-2019-9814	CVE-2019-11691	CVE-2019-11699	CVE-2019-11711	CVE-2019-11719	CVE-2019-11729
CVE-2019-9815	CVE-2019-11692	CVE-2019-11700	CVE-2019-11712	CVE-2019-11720	CVE-2019-11730
CVE-2019-9816	CVE-2019-11693	CVE-2019-11701	CVE-2019-11713	CVE-2019-11721	
CVE-2019-9817	CVE-2019-11694	CVE-2019-11702	CVE-2019-11714	CVE-2019-11723	
CVE-2019-9818	CVE-2019-11695	CVE-2019-11707	CVE-2019-11715	CVE-2019-11724	

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 July 2019 Security Patch Update (including Java 8 Update 201 software, and Firefox v68.0.1 Patches) is available for the FreeFlow® Print Server v2 Software Release running on Windows® v7 OS. The FreeFlow® Print Server software releases tested with the July 2019 Security Patch Update installed per printer products is illustrated below:

Printer Product	Patch Update Tested Releases
Color C60/C70 Printer	CP.20.1.17165.0
	CP.22.1.18064.1
IGen5 Press	CP.23.0.18058.0
Brenva™ Printer	CP.22.1.18064.0
	CP.22.1.18185.0

We have not tested the July 2019 Security Patch Update on all earlier FreeFlow® Print Server v2 releases, but there should not be any problems on those releases.

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 (DVD/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 DVD/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 DVD/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 end-points, 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 DVD/USB media may be more desirable for these highly Security sensitive customers. They can perform a Security scan of the DVD/USB media with a virus protection application prior to install. If the customer does not allow use of DVD/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., DVD/UB).

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., **July 2019 Security Patch Update for FFPS v2**) 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 end-points, and patch data transfer.

3.2 DVD/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 or ISO image file, 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 DVD/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 DVD/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 Update File	Windows® File Size (Kb)	Size in Bytes
FFPSv2-Win7_SecPatchUpdate_Jul2019.zip	3,313,954	3,393,488,580
FFPSv2-Win7_SecPatchUpdate_Jul2019.iso	3,314,304	3,393,847,296

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® 7 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 DVD/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.