Xerox Security Bulletin XRX17-009

Xerox® FreeFlow® Print Server v2 Integrated

Supports Xerox® Color C60/C70 Printer Products

April 2017 Security Patch Update

Bulletin Date: May 17, 2017

A. 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 2.0 / Windows v7 Integrated platform.

The FreeFlow® Print Server organization delivers Security Patch Updates on the FreeFlow® Print Server 2.0 / Windows v7 Integrated 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 C80/C70 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 2017 Security Patch Update
   - This supersedes the January 2017 Security Patch Update

Note: This April 2017 Security Patch Updates includes patch KB4012212 to mitigate the Wanna Decryptor ransomware worm. This extremely high severity worm has been pervasive and widely spread around the globe.

Remediated US-CERT Security Common Vulnerability Exposures (CVE's)					
CVE-2017-0001	CVE-2017-0009	CVE-2017-0045	CVE-2017-0056	CVE-2017-0084	CVE-2017-0147
CVE-2017-0004	CVE-2017-0022	CVE-2017-0047	CVE-2017-0059	CVE-2017-0086	
CVE-2017-0005	CVE-2017-0025	CVE-2017-0050	CVE-2017-0072	CVE-2017-0087	
CVE-2017-0008	CVE-2017-0039	CVE-2017-0055	CVE-2017-0083	CVE-2017-0088	

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.

B. Applicability

This April 2017 Security Patch Update is available for the FreeFlow® Print Server v2.0 Software Release running on Windows Embedded Standard v7 (WES7) Integrated OS.

i. 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 FreeFlow® Print Server Update Manager (GUI-based application) makes it simple for a customer to install Security patch updates. Downloading and installing Security Patch Updates using the FreeFlow® Print Server 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 v7 OS. 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.

ii. 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. 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 SSL over port 443 with the Xerox server.

Delivery and install of the Security Patch Update using FreeFlow® Print Server 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 installed.

C. 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.

See a more detailed description of the Security Patch Update delivery methods with the information below:

i. FreeFlow Print Server Update Manager Delivery

FFPS Update Manager is a GUI tool on the FFPS DFE used to check for Security updates, download Security updates, and install Security updates. The customer can install quarterly FFPS Security Patch Updates using the FFPS 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 FFPS 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 FFPS Security Patch Update should be listed (E.g., "April 2017 Security Patch Update for FFPS v2 Integrated") 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 FreeFlow® Print Server Update Manager UI to download and install on the FreeFlow® Print Server platform.

The customer proxy information is required to be setup on the FFPS platform so it can access to the Security Patch Update over the Internet. The FFPS platform initiates a "secure" communication session with the Xerox patch server using HTTP over the TSL 1.2 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, and SHA1 encryption. This connection ensures authentication of the FFPS 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 FFPS platform behind the customer firewall. The Xerox server and FFPS system both authenticate each other before making a connection between the two end-points, and patch data transfer.

ii. DVD/USB Media Delivery

Xerox uploads the FreeFlow® Print Server Security Patch Update to the Customer Field Operations (CFO) Web 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 include 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 the FreeFlow® Print Server Update Manger.

See the Security Patch Update deliverable filenames and sizes in the table below:

Security Patch Update File	Windows File Size (Kb)
FFPSv2.0Integrated_SecPatchUpdate_Apr2017.zip	1,049,172
FFPSv2.0Integrated_SecPatchUpdate_Apr2017.iso	1,049,522

iii. 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.

D. 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.