May 23, 2016

Xerox Security Bulletin XRX16-011

FreeFlow® Print Server v2.0 / Windows 7 Integrated
Supports C60/70 Printer Products

- April 2016 Security Patch Update

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 FFPS 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 FFPS 2.0 / Windows 7 Integrated platform.

The FFPS organization delivers Security Patch Updates on the FFPS 2.0 / Windows v7 Integrated platform by the FFPS organization on a quarterly (i.e., 4 times a year) basis. The FFPS engineering team receives new patch updates in January, April, July and October, and will test them for supported Printer products (such as C60/C70 printers) prior to delivery for customer install.

This bulletin announces the availability of the following:

- April 2016 Security Patch Update
  - ✓ This supersedes the January 2015 Security Patch Update

The Security vulnerabilities that are remediated with this FFPS Security patch delivery are as follows:

CVE-2009-2524	CVE-2015-6096	CVE-2016-0091	CVE-2016-0120	CVE-2016-0145	CVE-2016-0160
CVE-2013-3200	CVE-2015-6099	CVE-2016-0092	CVE-2016-0121	CVE-2016-0147	CVE-2016-0164
CVE-2015-2472	CVE-2016-0036	CVE-2016-0099	CVE-2016-0128	CVE-2016-0153	CVE-2016-0166
CVE-2015-2473	CVE-2016-0041	CVE-2016-0101	CVE-2016-0132	CVE-2016-0154	

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.

B. Applicability

This April 2016 Security Patch Update is available for the FFPS v2.0 Software Release running on Windows Embedded Standard 7 (WES7) Integrated OS.

The Security Patch Cluster made available over the network from a Xerox server using an application called FFPS Update Manager. The use of FFPS 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 FFPS Security Patch Update is available for delivery using media (DVD/USB) install. The FFPS customer schedules a Xerox Analyst or Xerox Service Engineer (CSE) to install the Security Patch Update at the customer account. The Analyst/CSE can decide if they allow a customer to install the Security Patch Updates.

Security of the network, devices and information on a customer network may be a consideration when deciding whether to use the DVD/USB or FFPS Update Manage method of delivering and installing Security Patch Updates. The external Xerox server that includes the Security Patch Update does not have access to the FFPS DFE platform at a customer site. The FFPS DFE platform (using Update Manager) initiates all communication to download the FFPS Security Patch Update, and the communication is "secure" by SSL over port 443. Delivery and install of the Security Patch Update using DVD/USB media can be an issue for some highly "secure" customer locations such as US Federal and State Government sites. An alternative method to delivery of the patch files is using secure transfer to the FFPS platform with transfer protocols such as "secure" FTP (SFTP) or "secure" Copy (SCP).

C. Patch Install

Xerox strives to deliver these critical Security patch updates in a timely manner. The customer process to obtain FFPS Security Patch Updates (delivered on a quarterly basis) is to contact the Xerox hotline support number. The two methods of FFPS Security Patch Update delivery and install are over the network (i.e., FFPS Update Manager) or from media (i.e., DVD/USB). See a more detailed description of the two Security Patch Update delivery methods with the information below:

i. FFPS Update Manager Delivery

Xerox uploads the FreeFlow Print Server Security Patch Update to a Xerox patch server that is available to the Internet outside of 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 FFPS Update Manager UI to download and install on the FFPS system. One requirement to access or connect to the Xerox patch sever over the network is configuration of the proxy information for the customer network. The FreeFlow Print Server Update Manager UI offers a 'Check for Updates' button selection to retrieve a list of patches. The Security Patch Update (April 2016 Security Patch Update) will be listed as a patch available for install. Downloading and installing the Security Patch Update is very simple with the FFPS Update Manager UI.

The FreeFlow Print Server (FFPS) Update Manager delivery of Windows Security Patch Update provides the ability to install Security patches on top of a pre-installed FFPS software release. The advantage of this Security install method delivery is the "ease of deliver and install" of this network delivery. Xerox has uploaded the quarterly FFPS v2.0 Security Patch Update to the external Xerox Server accessible over the Internet. An "Update Manger Patch Install" document (i.e., named FFPSv2Integrated_SecPatchUpdate_UM_May2016.pdf) is available with the information and procedures to complete the FFPS Security Patch Update install.

ii. DVD/USB Media Delivery

Xerox uploads the FreeFlow Print Server Security Patch Update to a Customer Field Operations (CFO) Web site that is available to the Xerox Analyst and Service once the deliverable has been tested and approved. The FreeFlow Print Server patch deliverable is a ZIP archive or ISO image, 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 FFPS software release. The install script include options to install the Security Patch Update directly from DVD/USB media or from the FFPS internal hard disk. A "FreeFlow Print Server DVD/USB Media Patch Install" document (i.e., named FFPSv2Integrated_SecPatchUpdate_DvdUsb_May2016.pdf) is available with the information and procedures to complete the FFPS Security Patch Update install.

If the Analyst supports their customer performing the Security Patch Update, then they must provide the customer with this document and the Security update deliverables identified in this document. This method of Security Patch Update install is not as convenient or simple for customer install as the network install method offered by the FFPS Update Manger.

We recommend the customer use the FFPS Update Manager 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 Updates, or they are not comfortable providing a network tunnel to the Xerox server that has the Security Patch Update. Therefore, this media install method is the best option under those circumstances.

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

Security Patch Update File	Windows File Size (Kb)
FFPSv2.0Integrated_SecPatchUpdate_Jan2016.zip	880,146
FFPSv2.0 Integrated _SecPatchUpdate_Jan2016.iso	880.496

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.