March 22, 2016

Xerox Security Bulletin XRX16-005 V1.0

FreeFlow® Print Server v2.0 / Windows 7 Integrated

Supports C60/70 Printer Products

- January 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.

Security patches are delivered for update on the FFPS 2.0 / Windows 7 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:

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

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

CVE-2011-0032
CVE-2011-0042
CVE-2011-1265
CVE-2013-0073
CVE-2013-3128
CVE-2013-3128
CVE-2013-3129
CVE-2013-3131
CVE-2013-3132
CVE-2013-3133
CVE-2013-3134
CVE-2013-3171
CVE-2013-3178
CVE-2013-3200
CVE-2013-3879
CVE-2013-3879
CVE-2013-3880
CVE-2013-3888
CVE-2013-3894
CVE-2013-3918
CVE-2014-0263
CVE-2014-0295
CVE-2014-0296
CVE-2014-1806
CVE-2014-1811
CVE-2014-2781
CVE-2014-4062
CVE-2014-4062
CVE-2014-4072
CVE-2014-4072
CVE-2014-4073
CVE-2014-4073
CVE-2014-4077
CVE-2014-4149
CVE-2014-6318
CVE-2014-6321
CVE-2014-6321
CVE-2014-6324
CVE-2014-6352
CVE-2015-0004
CVE-2015-0006
CVE-2015-0009
CVE-2015-0016
CVE-2015-0076
CVE-2015-0080
CVE-2015-0084
CVE-2015-0096
CVE-2015-0098
CVE-2015-1635
CVE-2015-1643
CVE-2015-1648
CVE-2015-1673
CVE-2015-1673
CVE-2015-1687
CVE-2015-1702
CVE-2015-1716
CVE-2015-1728
CVE-2015-1756
CVE-2015-1769
CVE-2015-2368
CVE-2015-2371
CVE-2015-2373
CVE-2015-2416
CVE-2015-2423
CVE-2015-2428
CVE-2015-2432
CVE-2015-2432
CVE-2015-2434
CVE-2015-2472
CVE-2015-2476
CVE-2015-2506
CVE-2015-2506
CVE-2015-2510
CVE-2015-2515
CVE-2015-2515
CVE-2015-2524
CVE-2015-2527
CVE-2015-2529
CVE-2015-6096
CVE-2015-6097
CVE-2015-6098
CVE-2015-6106
CVE-2015-6128
CVE-2015-6130
CVE-2015-6132
CVE-2016-0006
CVE-2016-0008
CVE-2016-0019
CVE-2016-0019
CVE-2016-0019
CVE-2016-0033
CVE-2016-0033
CVE-2016-0038
CVE-2016-0040
CVE-2016-0048
CVE-2016-0051
CVE-2016-0059
CVE-2016-0060
CVE-2016-0061
CVE-2016-0062
CVE-2016-0063
CVE-2016-0067
CVE-2016-0068
CVE-2016-0069
CVE-2016-0072
CVE-2016-0077

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

These updates are delivered over the network from a Xerox server using an application called FFPS Update Manager. The use of FFPS Update Manager makes it simple for a customer to install Security patch updates. The advantage of this Security patch update install method is the "ease of deliver and install" via the Update Manager UI, and access of the Security Patch Update over the network. In addition, the FFPS Security Patch Update is available for delivery using media (DVD/USB) install which can be performed by Xerox Service, and most likely the Analyst that supports a customer account. A customer performing this method of Security Patch Update is the decision of the CSE/Analyst that supports a customer.

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. All communication to download the FFPS Security Patch Update is initiated by the FFPS DFE platform, and the communication is "Secure" by SSL over port 443. If a DVD/USB media is restricted from a customer location such as with Government agencies, then Security Patch Update can be transferred to the FFPS system using a "secure" utility such as SFTP or SCP, and then installed.

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). Information for these two delivery and install methods are described below:

i. FFPS Update Manager Delivery

Once a quarterly Security Patch Update is ready for delivery, it is uploaded to a Xerox server that is available to the Internet outside of Xerox. 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. The customer network proxy information must be configured on the FFPS system so that it can connect to the Xerox server and get a list of available patches. Once the proxy information is configured, the Update Manager UI can be launched, and a button selected to get a list of available patch updates for the FFPS system. The Security Patch Update (January 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. The quarterly FFPS v2.0 Security Patch Update is uploaded to an external Xerox Server accessible over the Internet. A "Update Manger Patch Install" document (i.e., **FFPSv2Integrated_SecPatchUpdate_UM_Mar2016.pdf**) is available with the information and procedures to complete the FFPS Security Patch Update install.

ii. DVD/USB Media Delivery

Once the Security patch updates are ready for customer delivery they are made available on the FFPS Customer Field Operations (CFO) Web site. The FFPS Security Patch Update is delivered as an ISO image and ZIP archive file to provide the Xerox CSE/Analyst options to choose an install method. A script is provided that is executed to perform the Security Patch Update install, and can be installed on top of a pre-installed FFPS software release. The Security Patch Update and install scripts can be installed directly from the DVD/USB media, or copied to the FFPS DFE hard disk and then installed. A "DVD/USB Media Patch Install" document (i.e., **FFPSv2Integrated_SecPatchUpdate_DvdUsb_Mar2016.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.

If the customer wishes to install the FFPS Security Patch Update, then it is recommended that the FFPS Update Manager method be used. 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.

The Security Patch Update deliverable filenames and sizes are illustrated in the table below:

Security Patch Update File	Windows File Size (Kb)
FFPSv2.0Integrated_SecPatchUpdate_Jan2016.zip	650.210
FFPSv2.0 Integrated _SecPatchUpdate_Jan2016.iso	650.560

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.