November 21, 2016

Xerox Security Bulletin XRX16-027

FreeFlow® Print Server v2.1 / Windows v7 Standalone
Supports iGen®5 Printer Products

- October 2016 Security Patch Update
- Includes Java 8 Update 112, and Firefox v49.0 Patches

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 2.1 / Windows v7 Standalone platform.

The FFPS organization delivers Security Patch Updates on the FFPS 2.1 / Windows v7 Standalone 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 iGen®5 printers) prior to delivery for customer install.

Xerox tests FFPS 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. The Xerox support team can suggest options to minimize the risk of FFPS operation problems that could result from patch updates.

This bulletin announces the availability of the following:

1. October 2016 Security Patch Update
   - ✓ This supersedes the July 2016 Security Patch Update
2. Java 8 Update 112 Software
   - ✓ This supersedes Java 8 Update 102
3. Firefox 49.0 Patches

This patch deliverable remediates the US-CERT announced Security vulnerabilities below:

CVE-2015-2504	CVE-2016-3210	CVE-2016-3276	CVE-2016-3354	CVE-2016-3396	CVE-2016-5280
CVE-2016-0169	CVE-2016-3211	CVE-2016-3288	CVE-2016-3354	CVE-2016-5256	CVE-2016-5281
CVE-2016-0170	CVE-2016-3212	CVE-2016-3290	CVE-2016-3355	CVE-2016-5257	CVE-2016-5282
CVE-2016-0174	CVE-2016-3240	CVE-2016-3292	CVE-2016-3355	CVE-2016-5270	CVE-2016-5283
CVE-2016-0185	CVE-2016-3241	CVE-2016-3305	CVE-2016-3368	CVE-2016-5271	CVE-2016-5284
CVE-2016-0188	CVE-2016-3242	CVE-2016-3306	CVE-2016-3371	CVE-2016-5272	CVE-2016-5542
CVE-2016-0194	CVE-2016-3243	CVE-2016-3321	CVE-2016-3373	CVE-2016-5273	CVE-2016-5554
CVE-2016-0196	CVE-2016-3245	CVE-2016-3324	CVE-2016-3375	CVE-2016-5274	CVE-2016-5556
CVE-2016-0199	CVE-2016-3255	CVE-2016-3345	CVE-2016-3375	CVE-2016-5275	CVE-2016-5568
CVE-2016-0200	CVE-2016-3261	CVE-2016-3345	CVE-2016-3383	CVE-2016-5276	CVE-2016-5573
CVE-2016-2827	CVE-2016-3262	CVE-2016-3348	CVE-2016-3384	CVE-2016-5277	CVE-2016-5582
CVE-2016-3204	CVE-2016-3263	CVE-2016-3348	CVE-2016-3385	CVE-2016-5278	CVE-2016-5597
CVE-2016-3209	CVE-2016-3270	CVE-2016-3353	CVE-2016-3393	CVE-2016-5279	CVE-2016-7182

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 without not tested by Xerox.

B. Applicability

This October 2016 Security Patch Update (including Java 8 Update 112 software, and Firefox v49.0 Patches) is available for the FFPS v2.1 Software Release running on Windows v 7 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 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 method using media (DVD/USB) for the 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 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 FFPS 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, FFPS 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 FFPS 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 with the Xerox server.

Delivery and install of the Security Patch Update using FFPS 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, the Security Patch Update can be transferred (using SMB, SFTP, or SCP) to the FFPS 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 FFPS Security Patch Updates (delivered on a quarterly basis) is to contact the Xerox hotline support number. The methods of FFPS Security Patch Update delivery and install are over the network (i.e., FFPS Update Manager), from media (i.e., DVD/USB), or a customer can choose to install Security Patch Updates directly from Microsoft using Windows Update service.

We recommend the customer use the FFPS 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. Therefore, this 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. FFPS Update Manager Delivery

Xerox uploads the FFPS 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 FFPS Update Manager UI to download and install on the FFPS platform. 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 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. Downloading and installing the Security Patch Update is very simple with the FFPS Update Manager UI. Customers can choose the FFPS Update Manager method to manage Security Patch Update installs, and not require Xerox Service.

The FFPS Update Manager UI offers a 'Check for Updates' button selection to retrieve a list of patches. If the FFPS Update Manager displays a Security Patch Update in the list of patches it qualifies for install on the local FFPS platform. There are UI buttons to download and then install the patches. Xerox has uploaded the quarterly FFPS v2.1Security Patch Update to the external Xerox Server accessible over the Internet. A document named **FFPSv2Standalone_SecPatchUpdate_UM_Oct2016.pdf** is available as an Install Guide for the FFPS Update Manager.

ii. DVD/USB Media Delivery

Xerox uploads the FFPS 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 FFPS patch deliverables are 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 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 **FFPSv2Standalone_SecPatchUpdate_DvdUsb_Oct2016.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. 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.

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

Security Patch Update File	Windows File Size (Kb)
FFPSv2.1Standalone_SecPatchUpdate_Oct2016.zip	717.451
FFPSv2.1Standalone_SecPatchUpdate_Oct2016.iso	717.802

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 computers 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 FFPS platform. It is required that the customer proxy server information be configured on the FFPS 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 FFPS 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 FFPS system recovery if the installed Security patches creates a software problem or results in the FFPS software becoming inoperable. The Security Patch Update makes changes to only the Windows 7 OS system, and not the FFPS 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 FFPS System Restore. We recommend performing a full FFPS System Backup for redundancy purposes in case the checkpoint restore does not work. The only option for FFPS system recovery may be the FFPS System Backup if the system should become inoperable such that Windows is not stable. Make sure to store the FFPS System backup onto a remove 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.