Xerox Security Bulletin XRX19-006

Xerox® FreeFlow® Print Server v9 / Solaris® 11

Supports:

- Xerox® Color 800i/1000i Digital Press
- Xerox® Versant® 3100 Press

Delivery of: January 2019 Security Patch Cluster
Includes: Java 7 Update 211
Bulletin Date: February 22, 2019

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements for the Solaris® Operating System platform. Oracle® does not provide these patches to the public, but authorize vendors like Xerox® to deliver them to customers with an active FreeFlow® Print Server Support Contracts (FSMA). Customers who may have an Oracle® Support Contract for their non-FreeFlow® Print Server / Solaris® Servers should not install patches not prepared/delivered by Xerox®. Installing non-authorized patches for the FreeFlow® Print Server software violates Oracle® agreements, can render the platform inoperable, and result in downtime and/or a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **January 2019 Security Patch Cluster**
   - Supersedes October 2018 Security Patch Cluster.
   - October 2017 Security Patch Cluster install is prerequisite.
   - October 2018 Security Patch Cluster install is prerequisite.
2. **Java 7 Update 211 Software**
   - Supersedes Java 7 Update 201 software.
3. **Firefox 52.9.0 Software**
   - Same version delivered with previous October 2018 Security Patch Cluster.

Note: Solaris® 11.2 is the base OS installed for the Xerox® Color 800i/1000i Press and requires upgrade to the Solaris® 11.3 OS before installing the January 2019 Security Patch Cluster. This upgrade is not required for the Xerox® Versant® 3100 Press given the base OS is already Solaris® 11.3. The October 2017 and October 2018 Security Patch Clusters are prerequisites before installing the January 2019 Security Patch Cluster.

See US-CERT Common Vulnerability Exposures (CVE) patches installed with Solaris® 11.3 OS Upgrade that are remediated in the table below:

Solaris® 11.3 Included Security Patch Remediated US-CERT CVE's					
CVE-2013-6370	CVE-2015-1819	CVE-2015-2729	CVE-2015-2737	CVE-2015-2922	CVE-2016-0414
CVE-2013-6371	CVE-2015-2721	CVE-2015-2730	CVE-2015-2738	CVE-2015-2923	CVE-2016-0416
CVE-2014-2653	CVE-2015-2722	CVE-2015-2731	CVE-2015-2739	CVE-2015-3900	CVE-2016-0418
CVE-2014-3564	CVE-2015-2724	CVE-2015-2733	CVE-2015-2740	CVE-2015-4020	CVE-2016-0419
CVE-2014-3566	CVE-2015-2725	CVE-2015-2734	CVE-2015-2741	CVE-2015-4920	CVE-2016-0426
CVE-2014-3634	CVE-2015-2726	CVE-2015-2735	CVE-2015-2742	CVE-2015-5600	CVE-2016-0431
CVE-2014-3683	CVE-2015-2728	CVE-2015-2736	CVE-2015-2743	CVE-2016-0403	CVE-2017-10003

See US-CERT Common Vulnerability Exposures (CVE) list for the January 2019 Security Patch Cluster below:

January 2019 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2017-12176	CVE-2017-12179	CVE-2017-12182	CVE-2017-12185	CVE-2018-0732	CVE-2018-0737
CVE-2017-12177	CVE-2017-12180	CVE-2017-12183	CVE-2017-12186	CVE-2018-0734	CVE-2018-5407
CVE-2017-12178	CVE-2017-12181	CVE-2017-12184	CVE-2017-12187	CVE-2018-0735	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 211 software remediate in table below:

Java 7 Update 211 Software Remediated US-CERT CVE's		
CVE-2018-11212	CVE-2019-2422	CVE-2019-2426

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v52.9.0 Software below:

Firefox v52.9.0 Software Remediated US-CERT CVE's					
CVE-2018-12359	CVE-2018-12364	CVE-2018-5150	CVE-2018-5157	CVE-2018-5174	CVE-2018-6126
CVE-2018-12360	CVE-2018-12365	CVE-2018-5154	CVE-2018-5158	CVE-2018-5178	
CVE-2018-12362	CVE-2018-12366	CVE-2018-5155	CVE-2018-5159	CVE-2018-5183	
CVE-2018-12363	CVE-2018-12368	CVE-2018-5156	CVE-2018-5168	CVE-2018-5188	

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 Cluster. Alternatively, the customer can install the Security Patch Cluster using the Update Manager UI from the Xerox® FreeFlow® Print Server Platform.

2.0 Applicability

The customer can schedule a Xerox Service or Analyst representative to deliver and install the Security Patch Cluster from the Update Manager UI, USB/DVD media or the hard disk on the FreeFlow® Print Server platform. A customer can work with the Xerox CSE/Analyst to install the quarterly Security Patch Clusters if they have the expertise. The Xerox CSE/Analyst would be required to provide the Security Patch Cluster deliverables if they agree to allow their customer install.

The January 2019 Security Patch Cluster is available for the FreeFlow® Print Server v9 release on the Solaris® 11.3 OS for the Xerox® printer products below:

1. Xerox® Color 800i/1000i Press
2. Xerox® Versant® 3100 Press

This Security patch deliverables have been tested on the FreeFlow® Print Server 93.I0.04A.S11 software release. We have not tested the January 2019 Security Patch Cluster on all earlier FreeFlow® Print Server 9.3 releases, but there should not be any problems on these releases.

Solaris® 11.2 is the base Operating System installed by default for the Xerox® Color 800i/1000i Press and requires upgrade to the Solaris® 11.3 OS before installing the January 2019 Security Patch Cluster. This upgrade is not required for the Xerox® Versant® 3100 Press given the base OS is already Solaris® 11.3. If the October 2017 Security Patch Cluster or later had already been installed, then the Solaris® 11.3 OS would already be installed on the platform as well.

In addition, it is a prerequisite to install the October 2017 and October 2018 Security Patch Clusters on the FreeFlow® Print Server platform before installing the January 2019 Security Patch Cluster. A patch version script is provided to assist with identification of the current Security Patch Cluster version installed as well as other version information (E.g., Solaris® OS). If the script output illustrates that the January 2018 Security Patch Cluster (or newer version) is installed it means that the October 2017 Security Patch Cluster has already been installed, so that prerequisite is satisfied. If the currently installed Security Patch Cluster is an older version than October 2018, then the October 2018 Security Patch Cluster prerequisite must be installed prior to installing the January 2019 Security Patch Cluster.

Xerox® offers the Security Patch Cluster 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. The January 2019 Security Patch Cluster is delivered for install from the Update Manager UI given the smaller size compared to previous Security Patch Cluster versions. The Solaris® 11.3 OS upgrade, October 2017and 2018 Security Patch Clusters are too large to be supported by Update Manager. These larger deliverables can be transported to the customer location on DVD/USB media, or a laptop computer hard drive, and installed from a directory location on the FreeFlow Print Server platform. As a result of their large size, we delivered the Solaris 11.3 OS upgrade as two-part ZIP files, and the October 2017 and October 2018 Security Patch Clusters as three-part ZIP files. They can be transferred to the FreeFlow Print Server over the network using SFTP, or copied from USB media to prepare for install.

The Update Manager UI delivery of the Security Patch Cluster provides the ability to install Security patches on top of a pre-installed FreeFlow® Print Server software release. The advantage of this network install method is the "ease of delivery and install" from a Xerox patch server over the Internet. This easy install method gives a FreeFlow® Print Server customer the option to manage quarterly Security Patch Cluster install without need for support from Xerox service. This empowers the customer to have the option of installing 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 Cluster or they are not comfortable providing a network tunnel to the Xerox® Xerox® communication server that stores Security patches. In this case, the media install method (i.e., USB/DVD, hard drive) is the best option under those circumstances.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool that enables identification of the currently installed Solaris® OS version, FreeFlow® Print Server software version, Security Patch Cluster version, Java Software version and identification if the Solaris 11.3 Base Repository has been installed. This tool can be initially run to determine of the prerequisite Solaris® 11.3 OS and October 2017 Security Patch Cluster are currently installed. Example output from this script for the FreeFlow® Print Server v9 software is as follows:

Solaris® OS Version:	11.3
FFPS Release Version	9.0_SP-3_(93.I0.04A.86)
FFPS Patch Cluster	January 2019
Java Version	Java 7 Update 211
Base Repository	Installed

The above versions are the correct information after installing the January 2019 Security Patch Cluster. The Base Repository is optional.

3.0 Patch Install

Xerox® strives to deliver critical Security patch updates in a timely manner. The customer process to obtain Security Patch Cluster updates (delivered on a quarterly basis) is to contact the Xerox hotline support number. Xerox Service or an analyst can install the Patch Cluster using a script utility that will support install over the network using the Update Manger UI on the FreeFlow® Print Server platform, or from USB/DVD media, or from the hard disk on the FreeFlow® Print Server platform.

The FreeFlow® Print Server v9 application is on top of the Solaris® 11.2 OS for the Color 800i/1000i Press after initial software install. Upgrade to the Solaris® 11.3 OS and install the October 2017 and October 2018 Security

Patch Clusters prior to installing the January 2019 Security Patch Cluster. Delivery of the Solaris® 11.3 OS upgrade includes ZIP files as part 1 and part 2 to address file size issues. Once the patch cluster has been prepared on USB/DVD media or the hard disk on the FreeFlow® Print Server platform, a script is run to perform the Solaris 11.3 OS upgrade install.

3.1 DVD/USB Delivery and Install Method

The Security Patch Cluster deliverables are available on a secure FTP site once they are ready for customer delivery. The Xerox CSE/Analyst can download and prepare for the install by writing the Security patch update into a known directory on the FreeFlow® Print Server platform, or on DVD/USB media. Delivery of the Security Patch Cluster includes an ISO and ZIP archive file for convenience. Once the patch cluster has been prepared on media, run the provided install script to perform the install. The install script accepts an argument that identifies the media that contains a copy of the FreeFlow® Print Server Security Patch Cluster. (e.g., # installSecPatches.sh [disk | usb | dvd]).

Delivery of the January 2019 Security Patch Cluster includes a ZIP and ISO image file. The ISO image file can be written to DVD media to transport and install on the FreeFlow® Print Server platform. The ZIP file can be copied to a well-defined location on the FreeFlow® Print Server hard drive to prepare for install. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install. Alternatively, the January 2019 Security Patch Cluster can be installed from USB/DVD media. Make sure that the Color 800i/1000i Press is upgraded to the Solaris® 11.3 OS prior to installing the January 2019 Security Patch Cluster. The Solaris® 11.3 OS upgrade is not available using the Update Manager UI from the FreeFlow Print Server given the large size of the deliverable.

Note: The install of this Security Patch Cluster can fail if the archive file containing the software is corrupted from when downloading the deliverables from the SFTP site, copying them to USB media or uploading them to the hard drive on the FreeFlow® Print Server platform over a network connection. The table below illustrate file size on Windows®, file size on Solaris® and checksum on Solaris® for the January 2019 Security Patch Cluster files.

January 2019 Security Patch Cluster Files

Security Patch File	Windows® Size (Kb)	Solaris® Size (bytes)	Solaris® Checksum
Jan2019AndJava7Update211Patches_v9S11.zip	1,124,639	1,151,630,094	58468 2249278
Jan2019AndJava7Update211Patches_v9S11.iso	1,124,990	1,151,989,760	16654 2249980

Verify integrity of the Security Patch files from the FreeFlow® Print Server hard drive by comparing it to the original archive file size checksum with the actual checksum of these files on the platform. Change directory to the location of the Security Patch Cluster file and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., '**sum Jan2019AndJava7Update211Patches_v9S11.zip**'). The output of the '**sum**' command should match the checksum in the above table.

3.2 Update Manager UI Delivery and Install Method

Once Security patches are ready for customer delivery, they are available from the Xerox communication server. Procedures are available for the Customer or Xerox Service for using the Update Manager UI 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 communication server. When this option is selected the latest Security Patch Cluster should be listed (E.g., **January 2019 Security Patch Cluster for FFPS v9.3 / Solaris 11**) as available for download and install. The Update Manager UI includes mouse selectable buttons to download and then install the patches.

Xerox® uploads the Security Patch Cluster 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 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 communication server using HTTP over the TLS 1.0 protocol (HTTPS on port 443) using an RSA 2018-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 platform both authenticate each other before making a connection between the two end-points, and patch data transfer.

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.