Xerox Security Bulletin XRX18-019

Xerox® FreeFlow® Print Server v9 / Solaris® 11

Supports:

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

Delivery of: April 2018 Security Patch Cluster
Includes: Java 7 Update 181
Bulletin Date: May 31, 2018

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. **April 2018 Security Patch Cluster**
   - Supersedes January 2018 Security Patch Cluster.
   - October 2017 Security Patch Cluster install is prerequisite.
2. **Java 7 Update 181 Software**
   - Supersedes Java 7 Update 171 software.
3. **Solaris 11.3 Base Repository**
   - Only needed if customer use SMB for workflow (E.g., Hot Folder)
   - Allows update to Samba v4.4.16.

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 April 2018 Security Patch Cluster. This upgrade is not required for the Xerox® Versant® 3100 Press given the base OS is already Solaris® 11.3. Also, there are dependencies from the October 2017 Security Patch Cluster. If this dependency has not been previously installed, you must install it as a prerequisite to installing the April 2018 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) the April 2018 Security Patch Cluster remediate in table below:

April 2018 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2015-1315	CVE-2017-6259	CVE-2018-2583	CVE-2018-5127	CVE-2018-7054	CVE-2018-7329
CVE-2017-1000158	CVE-2017-6266	CVE-2018-2590	CVE-2018-5129	CVE-2018-7170	CVE-2018-7330
CVE-2017-17784	CVE-2017-6267	CVE-2018-2591	CVE-2018-5130	CVE-2018-7182	CVE-2018-7331
CVE-2017-17789	CVE-2017-7392	CVE-2018-2612	CVE-2018-5131	CVE-2018-7183	CVE-2018-7332
CVE-2017-3144	CVE-2017-7393	CVE-2018-2622	CVE-2018-5144	CVE-2018-7184	CVE-2018-7333
CVE-2017-3145	CVE-2017-7394	CVE-2018-2640	CVE-2018-5145	CVE-2018-7185	CVE-2018-7334
CVE-2017-3735	CVE-2017-7395	CVE-2018-2645	CVE-2018-5146	CVE-2018-7320	CVE-2018-7335
CVE-2017-3736	CVE-2017-7396	CVE-2018-2647	CVE-2018-5148	CVE-2018-7321	CVE-2018-7336
CVE-2017-3737	CVE-2018-1000031	CVE-2018-2665	CVE-2018-5732	CVE-2018-7322	CVE-2018-7337
CVE-2017-3738	CVE-2018-1000032	CVE-2018-2668	CVE-2018-5733	CVE-2018-7323	CVE-2018-7417
CVE-2017-5581	CVE-2018-1000033	CVE-2018-2696	CVE-2018-6836	CVE-2018-7324	CVE-2018-7418
CVE-2017-5715	CVE-2018-1000034	CVE-2018-2703	CVE-2018-7050	CVE-2018-7325	CVE-2018-7419
CVE-2017-5753	CVE-2018-1000035	CVE-2018-2764	CVE-2018-7051	CVE-2018-7326	CVE-2018-7420
CVE-2017-5754	CVE-2018-2562	CVE-2018-2808	CVE-2018-7052	CVE-2018-7327	CVE-2018-7421
CVE-2017-6257	CVE-2018-2573	CVE-2018-5125	CVE-2018-7053	CVE-2018-7328	

See the US-CERT Common Vulnerability Exposures (CVE) the Java 7 Update 181 Software remediate in table below:

Java 7 Update 181 Software Remediated US-CERT CVE's					
CVE-2018-2783	CVE-2018-2794	CVE-2018-2796	CVE-2018-2798	CVE-2018-2800	CVE-2018-2815
CVE-2018-2790	CVE-2018-2795	CVE-2018-2797	CVE-2018-2799	CVE-2018-2814	

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 USB media or the hard disk on the FreeFlow® Print Server. 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 customer install.

The April 2018 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 deliverable has been tested on the FreeFlow® Print Server 93.I0.04A.S11 software release. We have not tested the April 2018 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 for the Xerox® Color 800i/1000i Press and requires upgrade to the Solaris® 11.3 OS before installing the April 2018 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 had already been installed, then the Solaris® 11.3 OS would already be installed on the platform as well. If the January 2018 Security Patch Cluster had already been installed, then the October 2017 had already been installed given it was a prerequisite.

In addition, it is a prerequisite to install the October 2017 Security Patch Cluster on the FreeFlow® Print Server platform before installing the April 2018 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 is installed it means that the October 2017 Security Patch Cluster had already been installed, so the prerequisite is satisfied.

As a result of the very large file size of these deliverables, the download and install of the Solaris® 11.3 OS upgrade and April 2018 Security Patch Cluster are not supported from the Update Manager UI on the FreeFlow® Print Server platform. The April 2018 Security Patch Cluster is delivered as three-part ZIP files so that they can be transported on DVD/USB media, and installed from USB media or from a directory location on the FreeFlow Print Server platform. We delivered the Solaris 11.3 OS upgrade and October 2017 Security Patch Cluster as two-part ZIP files as a result of their large size. They can be transferred to the FreeFlow Print Server over the network using SFTP, or copied from USB media.

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	April 2018
Java Version	Java 7 Update 181
Base Repository	Not Installed

The above versions are the correct information after installing the April 2018 Security Patch Cluster.

We deliver a Base Repository software for the Solaris 11.3 OS with the delivery of the April 2018 Security Patch Cluster. You only need to install the Base Repository if interested in updating Samba from v3.6.25 to v4.4.16. If a customer is using SMB shares for any purpose (E.g., Hot Folder workflow) it is recommended to install the Base Repository to ensure Samba is updated to v4.4.16. The Base Repository software is a large package so delivered as three-part ZIP files.

3.0 Patch Install

Xerox® strives to deliver these 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 installing from USB 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 the October 2017 Security Patch Cluster is required prior to installing the April 2018 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 media or the hard disk on the FreeFlow® Print Server platform, a script is run to perform the install.

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 [diskl usb]).

Delivery of the April 2018 Security Patch Cluster includes ZIP files separated as three parts to address file size issues. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install. Make sure that the Color 800i/1000i Press is upgraded to the Solaris® 11.3OS prior to installing the April 2018 Security Patch Cluster. This delivery 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® checksum on Solaris® for the April 2018 Security Patch Cluster files.

April 2018 Security Patch Cluster Files

Security Patch File	Windows® Size (Kb)	Solaris® Size (bytes)	Solaris® Checksum
Apr2018AndJava7Update181Patches_v9S11-Part1.zip	3,169,173	3,245,232,720	24314 6338346
Apr2018AndJava7Update181Patches_v9S11-Part2.zip	3,463,036	3,546,148,321	3469 6926071
Apr2018AndJava7Update181Patches_v9S11-Part3.zip	1,318,059	1,349,692,153	53665 2636118

Verify integrity of the Security Patch ZIP files contained on 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 ZIP files and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., '**sum Apr2018AndJava7Update181Patches_v9S11-Part1.zip**'). The output of the 'sum' command should match the above table.

The table below illustrate file size on Windows® and file size on Solaris® and checksum on Solaris® for the Solaris® 11.3OS Base Repository files.

Solaris® 11.3 OS Base Repository Files

Security Patch File	Windows Size (K-bytes)	Solaris Size (bytes)	Solaris Checksum
Solaris11.3_Base_Repo_part1.zip	3,194,109	3270767004	13588 6388217
Solaris11.3_Base_Repo_part2.zip	3,374,944	3589100941	7577 7009963
Solaris11.3_Base_Repo_part3.zip	1,533,570	1570375293	15522 3067140

Verify integrity of the Solaris® 11.3 Base Repository ZIP files contained on the FreeFlow® Print Server hard drive by comparing it to the original archive file checksum with the actual checksum of these files on the platform. Change directory to the location of the Solaris® 11.3 Base Repository ZIP files and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., '**sum Solaris11.3_Base_Repo_part1.zip**'). The output of the 'sum' command should match the above table.

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.