Xerox Security Bulletin XRX18-012

Xerox® FreeFlow® Print Server v9 / Solaris® 11

Supports:

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

Delivery of: January 2018 Security Patch Cluster
Includes: Java 7 Update 171
Bulletin Date: April 3, 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. **Solaris® 11.3 Operating System (OS) Upgrade**
   - This supersedes the Solaris® 11.2 OS
   - Required for Color 800i/1000i Presses only.
   - Solaris® 11.3 OS already installed for the Xerox® Versant® 3100.
2. **January 2018 Security Patch Cluster**
   - Predecessor to the October 2017 Security Patch Cluster.
   - October 2017 Security Patch Cluster install is prerequisite.
3. **Java 7 Update 171 Software**
   - This supersedes Java 7 Update 161 software.

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.

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 January 2018 Security Patch Cluster remediate in table below:

January 2018 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2014-8127	CVE-2016-5323	CVE-2017-12901	CVE-2017-13024	CVE-2017-15189	CVE-2017-7601
CVE-2014-8128	CVE-2016-5875	CVE-2017-12902	CVE-2017-13025	CVE-2017-15190	CVE-2017-7602
CVE-2014-8129	CVE-2016-6223	CVE-2017-12985	CVE-2017-13026	CVE-2017-15191	CVE-2017-7793
CVE-2014-8130	CVE-2016-9273	CVE-2017-12986	CVE-2017-13027	CVE-2017-15192	CVE-2017-7805
CVE-2015-3193	CVE-2016-9296	CVE-2017-12987	CVE-2017-13028	CVE-2017-15193	CVE-2017-7810
CVE-2015-7554	CVE-2016-9297	CVE-2017-12988	CVE-2017-13029	CVE-2017-16548	CVE-2017-7814
CVE-2015-8870	CVE-2016-9318	CVE-2017-12989	CVE-2017-13030	CVE-2017-17083	CVE-2017-7818
CVE-2016-0701	CVE-2016-9532	CVE-2017-12990	CVE-2017-13031	CVE-2017-17084	CVE-2017-7819
CVE-2016-10092	CVE-2016-9533	CVE-2017-12991	CVE-2017-13032	CVE-2017-17085	CVE-2017-7823
CVE-2016-10093	CVE-2016-9534	CVE-2017-12992	CVE-2017-13033	CVE-2017-2753	CVE-2017-7824
CVE-2016-10094	CVE-2016-9535	CVE-2017-12993	CVE-2017-13034	CVE-2017-3142	CVE-2017-7825
CVE-2016-10095	CVE-2016-9536	CVE-2017-12994	CVE-2017-13035	CVE-2017-3143	CVE-2017-7826
CVE-2016-10207	CVE-2016-9537	CVE-2017-12995	CVE-2017-13036	CVE-2017-3651	CVE-2017-7828
CVE-2016-2334	CVE-2016-9538	CVE-2017-12996	CVE-2017-13037	CVE-2017-3652	CVE-2017-7829
CVE-2016-2335	CVE-2016-9539	CVE-2017-12997	CVE-2017-13038	CVE-2017-3653	CVE-2017-7830
CVE-2016-3186	CVE-2016-9540	CVE-2017-12998	CVE-2017-13039	CVE-2017-3731	CVE-2017-7843
CVE-2016-3619	CVE-2017-0379	CVE-2017-12999	CVE-2017-13040	CVE-2017-3732	CVE-2017-7845
CVE-2016-3620	CVE-2017-10155	CVE-2017-13000	CVE-2017-13041	CVE-2017-3735	CVE-2017-7846
CVE-2016-3621	CVE-2017-10227	CVE-2017-13001	CVE-2017-13042	CVE-2017-3736	CVE-2017-7847
CVE-2016-3622	CVE-2017-10268	CVE-2017-13002	CVE-2017-13043	CVE-2017-3737	CVE-2017-7848
CVE-2016-3623	CVE-2017-10276	CVE-2017-13003	CVE-2017-13044	CVE-2017-3738	CVE-2017-9117
CVE-2016-3624	CVE-2017-10279	CVE-2017-13004	CVE-2017-13045	CVE-2017-5225	CVE-2017-9526
CVE-2016-3625	CVE-2017-10283	CVE-2017-13005	CVE-2017-13046	CVE-2017-5563	CVE-2018-2560
CVE-2016-3631	CVE-2017-10286	CVE-2017-13006	CVE-2017-13047	CVE-2017-5715	CVE-2018-2577
CVE-2016-3632	CVE-2017-10294	CVE-2017-13007	CVE-2017-13048	CVE-2017-5753	CVE-2018-2578
CVE-2016-3633	CVE-2017-10314	CVE-2017-13008	CVE-2017-13049	CVE-2017-5754	CVE-2018-5089
CVE-2016-3634	CVE-2017-10378	CVE-2017-13009	CVE-2017-13050	CVE-2017-5969	CVE-2018-5091
CVE-2016-3658	CVE-2017-10379	CVE-2017-13010	CVE-2017-13051	CVE-2017-6257	CVE-2018-5095
CVE-2016-3945	CVE-2017-10384	CVE-2017-13011	CVE-2017-13052	CVE-2017-6259	CVE-2018-5096
CVE-2016-3990	CVE-2017-11108	CVE-2017-13012	CVE-2017-13053	CVE-2017-6266	CVE-2018-5097
CVE-2016-3991	CVE-2017-11541	CVE-2017-13013	CVE-2017-13054	CVE-2017-6267	CVE-2018-5098
CVE-2016-5102	CVE-2017-11542	CVE-2017-13014	CVE-2017-13055	CVE-2017-6508	CVE-2018-5099
CVE-2016-5314	CVE-2017-11543	CVE-2017-13015	CVE-2017-13089	CVE-2017-7592	CVE-2018-5102
CVE-2016-5315	CVE-2017-12893	CVE-2017-13016	CVE-2017-13090	CVE-2017-7593	CVE-2018-5103
CVE-2016-5316	CVE-2017-12894	CVE-2017-13017	CVE-2017-13687	CVE-2017-7594	CVE-2018-5104
CVE-2016-5317	CVE-2017-12895	CVE-2017-13018	CVE-2017-13688	CVE-2017-7595	CVE-2018-5117
CVE-2016-5318	CVE-2017-12896	CVE-2017-13019	CVE-2017-13689	CVE-2017-7596	CVE-2018-5334
CVE-2016-5319	CVE-2017-12897	CVE-2017-13020	CVE-2017-13690	CVE-2017-7597	CVE-2018-5335

CVE-2016-5320	CVE-2017-12898	CVE-2017-13021	CVE-2017-13725	CVE-2017-7598	CVE-2018-5336
CVE-2016-5321	CVE-2017-12899	CVE-2017-13022	CVE-2017-13726	CVE-2017-7599	
CVE-2016-5322	CVE-2017-12900	CVE-2017-13023	CVE-2017-13727	CVE-2017-7600	

See the US-CERT Common Vulnerability Exposures (CVE) the Java 7 Update 171 Software remediate in table below:

Java 7 Update 171 Software Remediated US-CERT CVE's					
CVE-2018-2579	CVE-2018-2599	CVE-2018-2618	CVE-2018-2634	CVE-2018-2657	CVE-2018-2678
CVE-2018-2581	CVE-2018-2602	CVE-2018-2629	CVE-2018-2637	CVE-2018-2663	
CVE-2018-2588	CVE-2018-2603	CVE-2018-2633	CVE-2018-2641	CVE-2018-2677	

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 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.

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 January 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. The January 2018 Security Patch Cluster is available for the FreeFlow® Print Server v9 release running on the Xerox® printer products below:

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

In addition, it is a prerequisite to install the October 2017 Security Patch Cluster on the FreeFlow® Print Server platform before installing the January 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). The output from this script is illustrated below in this section.

As a result of the very large file size of these deliverables, the download and install of the Solaris® 11.3 OS upgrade and January 2018 Security Patch Cluster are not supported from the Update Manager UI on the FreeFlow® Print Server platform. Therefore, it is required to deliver the Security Patch Cluster files on a laptop PC so they can be transferred over the customer network using SFTP to the FreeFlow® Print Server platform for install, or on USB media so the patches can be installed from the USB media, or copied to the FreeFlow® Print Server platform for install.

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, and Java Software version. 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 2018
Java Version	Java 7 Update 171

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

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 the Security Patch Cluster from USB media or from the hard disk on the FreeFlow® Print Server platform. The Security Patch Cluster deliverables are available on a secure FTP site once they are ready for customer delivery.

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 January 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.

Delivery of the Security Patch Cluster includes ZIP files separated as part 1, part 2 and part 3 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 January 2018 Security Patch Cluster.

Note: The install of this Security Patch Cluster and/or Solaris® 11 OS upgrade 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® and file size on Solaris® and checksum on Solaris® for the Solaris® 11.3OS upgrade files.

Solaris® 11.3 OS Upgrade Files (for Xerox® Color 800i/1000i Press only)

Security Patch File	Windows® Size (Kb)	Solaris® Size (bytes)	Solaris® Checksum
Sol-11.3_Upgrade_Part-1.zip	4,727,677	4.841,140,675	41735 9455353
Sol-11.3_Upgrade_Part-2.zip	3,504,985	3,589,103,767	56371 7009969

Verify integrity of the Solaris® 11.3 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 Solaris® 11.3 ZIP files and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., '**sum Sol-11.3_Upgrade_Part-1.zip**'). The output of the 'sum' command should match the above table.

The table below illustrate file size on Windows®, file size on Solaris® checksum on Solaris® for the January 2018 Security Patch Cluster files.

January 2018 Security Patch Cluster Files

Security Patch File	Windows® Size (Kb)	Solaris® Size (bytes)	Solaris® Checksum
Jan2018AndJava7Update171Patches_v9S11-Part1.zip	2,912,337	2,982,232,212	21636 5824673
Jan2018AndJava7Update171Patches_v9S11-Part2.zip	3,105,995	3,180,538,310	37005 6211989
Jan2018AndJava7Update171Patches_v9S11-Part3.zip	1,786,366	1,829,238,613	28081 3572732

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 Jan2018AndJava7Update171Patches_v9S11-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.