Xerox Security Bulletin XRX21-010

Xerox® FreeFlow® Print Server v7

For: Solaris® 11.4 Operating System
Install Method: DVD/USB Media
Supports: Xerox Nuvera® PSIP 14.3 Printer Products

Deliverable: April 2021 Security Patch Cluster
Includes: Java 7 Update 301
Bulletin Date: May 26, 2021

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 2021 Security Patch Cluster**
   - This is the first Security Patch Cluster for RV 14.3.18 / Solaris 11.4
   - There are no Security Patch Cluster prerequisites required.
2. **Java 7 Update 301 Software**
   - Supersedes Java 7 Update 291 Software
3. **Firefox 78.9.0 Software**
   - Supersedes Firefox 52.9.0

See US-CERT Common Vulnerability Exposures (CVE) the April 2021 Security Patch Cluster remediate in table below:

April 2021 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2019-17042	CVE-2020-13631	CVE-2020-14769	CVE-2020-14954	CVE-2020-26575	CVE-2020-8177
CVE-2016-10739	CVE-2020-13632	CVE-2020-14771	CVE-2020-15025	CVE-2020-2752	CVE-2020-8265
CVE-2018-20781	CVE-2020-13645	CVE-2020-14775	CVE-2020-15358	CVE-2020-27619	CVE-2020-8287
CVE-2018-7160	CVE-2020-13817	CVE-2020-14776	CVE-2020-15466	CVE-2020-2763	CVE-2020-8315
CVE-2018-8956	CVE-2020-13871	CVE-2020-14789	CVE-2020-15888	CVE-2020-2780	CVE-2020-8492
CVE-2019-1010180	CVE-2020-13962	CVE-2020-14790	CVE-2020-15889	CVE-2020-27814	CVE-2020-8618
CVE-2019-10197	CVE-2020-14093	CVE-2020-14793	CVE-2020-15900	CVE-2020-27841	CVE-2020-8619
CVE-2019-11135	CVE-2020-14154	CVE-2020-14809	CVE-2020-15945	CVE-2020-27842	CVE-2020-8620
CVE-2019-14869	CVE-2020-14318	CVE-2020-14812	CVE-2020-15999	CVE-2020-27843	CVE-2020-8621
CVE-2019-17040	CVE-2020-14323	CVE-2020-14814	CVE-2020-16117	CVE-2020-27844	CVE-2020-8622
CVE-2019-17041	CVE-2020-14344	CVE-2020-14827	CVE-2020-17489	CVE-2020-27845	CVE-2020-8623
CVE-2019-18348	CVE-2020-14345	CVE-2020-14828	CVE-2020-17498	CVE-2020-2804	CVE-2020-8624
CVE-2019-18634	CVE-2020-14346	CVE-2020-14829	CVE-2020-17507	CVE-2020-2812	CVE-2021-2001
CVE-2019-20044	CVE-2020-14347	CVE-2020-14830	CVE-2020-1967	CVE-2020-2814	CVE-2021-2010
CVE-2019-2007	CVE-2020-14361	CVE-2020-14837	CVE-2020-1971	CVE-2020-2922	CVE-2021-2011
CVE-2019-20079	CVE-2020-14362	CVE-2020-14839	CVE-2020-24342	CVE-2020-29385	CVE-2021-2014

CVE-2019-20892	CVE-2020-14363	CVE-2020-14845	CVE-2020-24369	CVE-2020-36221	CVE-2021-2022
CVE-2019-20907	CVE-2020-14422	CVE-2020-14846	CVE-2020-24370	CVE-2020-36222	CVE-2021-2032
CVE-2019-20919	CVE-2020-14539	CVE-2020-14852	CVE-2020-24371	CVE-2020-36223	CVE-2021-2060
CVE-2019-5068	CVE-2020-14540	CVE-2020-14860	CVE-2020-25219	CVE-2020-36224	CVE-2021-2192
CVE-2019-6706	CVE-2020-14547	CVE-2020-14861	CVE-2020-25692	CVE-2020-36225	CVE-2021-22173
CVE-2019-9740	CVE-2020-14550	CVE-2020-14866	CVE-2020-25862	CVE-2020-36226	CVE-2021-22174
CVE-2019-9947	CVE-2020-14553	CVE-2020-14867	CVE-2020-25863	CVE-2020-36227	CVE-2021-22191
CVE-2020-10531	CVE-2020-14559	CVE-2020-14868	CVE-2020-25866	CVE-2020-36228	CVE-2021-22883
CVE-2020-11080	CVE-2020-14576	CVE-2020-14869	CVE-2020-26116	CVE-2020-36229	CVE-2021-22884
CVE-2020-11736	CVE-2020-14672	CVE-2020-14870	CVE-2020-26137	CVE-2020-36230	CVE-2021-23336
CVE-2020-11868	CVE-2020-1472	CVE-2020-14871	CVE-2020-26154	CVE-2020-3909	CVE-2021-23840
CVE-2020-12049	CVE-2020-14754	CVE-2020-14873	CVE-2020-26418	CVE-2020-3910	CVE-2021-27212
CVE-2020-12825	CVE-2020-14758	CVE-2020-14878	CVE-2020-26419	CVE-2020-3911	CVE-2021-3156
CVE-2020-13434	CVE-2020-14759	CVE-2020-14891	CVE-2020-26420	CVE-2020-6750	CVE-2021-3177
CVE-2020-13435	CVE-2020-14760	CVE-2020-14893	CVE-2020-26421	CVE-2020-8172	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 301 software below:

Java 7 Update 301 Software Remediated US-CERT CVE's			
CVE-2021-2161	CVE-2021-2163		

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v78.9.0 software below:

Firefox v78.9.0 Software Remediated US-CERT CVE's					
CVE-2019-11734	CVE-2019-17002	CVE-2020-12417	CVE-2020-15656	CVE-2020-16044	CVE-2020-6514
CVE-2019-11735	CVE-2019-17013	CVE-2020-12418	CVE-2020-15657	CVE-2020-26950	CVE-2021-23953
CVE-2019-11736	CVE-2019-17014	CVE-2020-12419	CVE-2020-15658	CVE-2020-26951	CVE-2021-23954
CVE-2019-11737	CVE-2019-17018	CVE-2020-12420	CVE-2020-15659	CVE-2020-26953	CVE-2021-23960
CVE-2019-11738	CVE-2019-17019	CVE-2020-12421	CVE-2020-15663	CVE-2020-26956	CVE-2021-23964
CVE-2019-11741	CVE-2019-17020	CVE-2020-12422	CVE-2020-15664	CVE-2020-26958	CVE-2021-23968
CVE-2019-11747	CVE-2019-17023	CVE-2020-12423	CVE-2020-15670	CVE-2020-26959	CVE-2021-23969
CVE-2019-11748	CVE-2019-17025	CVE-2020-12424	CVE-2020-15673	CVE-2020-26960	CVE-2021-23973
CVE-2019-11749	CVE-2019-9232	CVE-2020-12425	CVE-2020-15676	CVE-2020-26961	CVE-2021-23978
CVE-2019-11750	CVE-2019-9235	CVE-2020-12426	CVE-2020-15677	CVE-2020-26965	CVE-2021-23981
CVE-2019-11751	CVE-2019-9325	CVE-2020-15648	CVE-2020-15678	CVE-2020-26966	CVE-2021-23982
CVE-2019-11754	CVE-2019-9371	CVE-2020-15652	CVE-2020-15683	CVE-2020-26968	CVE-2021-23984
CVE-2019-11756	CVE-2020-12402	CVE-2020-15653	CVE-2020-15969	CVE-2020-26971	CVE-2021-23987
CVE-2019-11765	CVE-2020-12415	CVE-2020-15654	CVE-2020-15999	CVE-2020-26976	
CVE-2019-17000	CVE-2020-12416	CVE-2020-15655	CVE-2020-16012	CVE-2020-6463	

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/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 April 2021 Security Patch Cluster is available for the FreeFlow® Print Server v7 / RV 14.3.18 release on the Solaris® 11.4 OS for the Xerox® printer products below:

1. Nuvera® 100/120/144/157 EA Digital Production System
2. Nuvera® 200/288/314 EA Perfecting Production System
3. Nuvera® 100/120/144 MX Digital Production System
4. Nuvera® 200/288 MX Perfecting Production System

This Security patch deliverable has been tested on the FreeFlow® Print Server 73.K5.22.11 software releases. The April 2021 Security Patch Cluster is the first installed for this new FFPS v7 / Solaris 11.4 configuration.

The April 2021 Security Patch Cluster is 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. There are four parts (4 ZIP files) delivered for this Security Patch Cluster. They can be transferred to the FreeFlow® Print Server over the network using SFTP or copied from USB/DVD media to prepare 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, Java Software version. This tool can be initially run to determine if the prerequisite October 2018 Security Patch Cluster is currently installed. Example output from this script for the FreeFlow® Print Server v7 software is as follows:

Solaris® OS Version:	11.4.32.88.3
FFPS Release Version	7.0_SP-3_(73.K5.22.11.86)
FFPS Patch Cluster	April 2021
Java Version	Java 7 Update 301

The above versions are the correct information after installing the April 2021 Security Patch Cluster.

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 from USB/DVD 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 Xerox CSE/Analyst can download and prepare for the install by transferring the Security patch update into a known directory on the FreeFlow® Print Server platform on to USB media. 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]).

Delivery of the April 2021 Security Patch Cluster includes four ZIP files. The ZIP files can be transferred 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 April 2021 Security Patch Cluster can be installed from USB media.

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 April 2021 Security Patch Cluster files.

April 2021 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Apr2021AndJava7Update301Patches_v7S11_4-Part1.zip	4,032,353	4,129,128,931	42644 8064705
Apr2021AndJava7Update301Patches_v7S11_4-Part2.zip	4,141,668	4,241,067,861	48910 8283336
Apr2021AndJava7Update301Patches_v7S11_4-Part3.zip	3,629,943	3,717,060,917	41444 7259885
Apr2021AndJava7Update301Patches_v7S11_4-Part4.zip	2,377,509	2,434,568,219	24498 4755017

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 Apr2021AndJava7Update301Patches_v7S11_4-Part1.zip**). The output of the '**sum**' command should match the checksum in 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.