Xerox Security Bulletin XRX22-005

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: January 2022 Security Patch Cluster
Includes: Java 7 Update 331
Bulletin Date: February 14, 2022

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 2022 Security Patch Cluster**
   - This Patch Cluster is only intended for FFPS v7 / RV 14.3.18 software release.

   Note: If the April 2021 Security Patch Cluster is currently installed a fresh FFPS v7 / RV 14.3.18 software scrape install is required. There is an issue installing the January 2022 Security Patch Cluster over top of the April 2021 Security Patch Cluster. It can be successfully installed over top of the July 2021 Security Patch Cluster and later.
2. **Java 7 Update 331 Software**
   - Supersedes Java 7 Update 321 Software
3. **Firefox 91.4.0esr Software**
   - Supersedes Firefox 78.11.0esr

See US-CERT Common Vulnerability Exposures (CVE) the January 2022 Security Patch Cluster remediate in table below:

January 2022 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2018-14339	CVE-2021-1817	CVE-2021-30665	CVE-2021-3497	CVE-2021-38508	CVE-2021-43537
CVE-2018-14340	CVE-2021-1820	CVE-2021-30666	CVE-2021-3498	CVE-2021-38509	CVE-2021-43538
CVE-2018-14341	CVE-2021-1825	CVE-2021-30682	CVE-2021-3516	CVE-2021-39920	CVE-2021-43539
CVE-2018-14342	CVE-2021-1826	CVE-2021-30689	CVE-2021-3517	CVE-2021-39921	CVE-2021-43541
CVE-2018-14343	CVE-2021-20254	CVE-2021-30720	CVE-2021-3518	CVE-2021-39922	CVE-2021-43542
CVE-2018-14344	CVE-2021-21775	CVE-2021-30734	CVE-2021-3522	CVE-2021-39923	CVE-2021-43543
CVE-2018-14367	CVE-2021-21779	CVE-2021-30744	CVE-2021-3537	CVE-2021-39924	CVE-2021-43545
CVE-2018-14368	CVE-2021-21806	CVE-2021-30749	CVE-2021-3541	CVE-2021-39925	CVE-2021-43546
CVE-2018-14369	CVE-2021-25219	CVE-2021-30758	CVE-2021-3580	CVE-2021-39926	CVE-2022-21263
CVE-2018-16056	CVE-2021-29981	CVE-2021-30761	CVE-2021-38502	CVE-2021-39928	CVE-2022-21298
CVE-2018-16057	CVE-2021-29982	CVE-2021-30762	CVE-2021-38503	CVE-2021-39929	CVE-2022-21375
CVE-2018-16058	CVE-2021-29987	CVE-2021-30795	CVE-2021-38504	CVE-2021-40528	CVE-2022-21384
CVE-2019-20388	CVE-2021-29991	CVE-2021-30797	CVE-2021-38505	CVE-2021-43395	

CVE-2020-24977	CVE-2021-30661	CVE-2021-30799	CVE-2021-38506	CVE-2021-43528	
CVE-2020-7595	CVE-2021-30663	CVE-2021-30858	CVE-2021-38507	CVE-2021-43536	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 331 software below:

Java 7 Update 331 Software Remediated US-CERT CVE's			
CVE-2022-21291	CVE-2022-21349		

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v91.4.0esr software below:

Firefox v91.4.0esr Software Remediated US-CERT CVE's					
CVE-2020-16042	CVE-2021-29967	CVE-2021-29991	CVE-2021-38501	CVE-2021-38509	CVE-2021-43543
CVE-2020-26950	CVE-2021-29980	CVE-2021-32810	CVE-2021-38503	CVE-2021-43536	CVE-2021-43545
CVE-2020-26968	CVE-2021-29981	CVE-2021-38495	CVE-2021-38504	CVE-2021-43537	CVE-2021-43546
CVE-2020-35113	CVE-2021-29982	CVE-2021-38496	CVE-2021-38505	CVE-2021-43538	
CVE-2021-23960	CVE-2021-29985	CVE-2021-38497	CVE-2021-38506	CVE-2021-43539	
CVE-2021-23964	CVE-2021-29987	CVE-2021-38498	CVE-2021-38507	CVE-2021-43541	
CVE-2021-29955	CVE-2021-29990	CVE-2021-38500	CVE-2021-38508	CVE-2021-43542	

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 January 2022 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 January 2022 Security Patch Cluster is the first installed for this new FFPS v7 / Solaris 11.4 configuration.

The January 2022 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. 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	January 2022
Java Version	Java 7 Update 331

The above versions are the correct information after installing the January 2022 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 January 2022 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 January 2022 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 January 2022 Security Patch Cluster files.

January 2022 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jan2022AndJava7Update331Patches_v7S11_4-Part1.zip	3,650,234	3,737,839,071	13374 7300467
Jan2022AndJava7Update331Patches_v7S11_4-Part2.zip	3,472,084	3,555,413,035	52478 6944167
Jan2022AndJava7Update331Patches_v7S11_4-Part3.zip	3,451,137	3,533,964,261	51396 6902274
Jan2022AndJava7Update331Patches_v7S11_4-Part4.zip	3,728,731	3,818,220,003	19121 7457461

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 Jan2022AndJava7Update331Patches_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.