Xerox Security Bulletin XRX21-017

Xerox® FreeFlow® Print Server v9

For: Solaris® 11.4 Operating System
Install Method: DVD/USB Media

Deliverable: July 2021 Security Patch Cluster
Includes: Java 7 Update 311
Bulletin Date: September 28, 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. **July 2021 Security Patch Cluster**
   - This Patch Cluster is only intended for the FFPS v93.K4.85 software release.
   - These Security patches are supported by the Solaris 11.4 OS only.
2. **Java 7 Update 311 Software**
   - Supersedes Java 7 Update 301 Software
3. **Firefox 78.11.0esr Software**
   - Supersedes Firefox 78.9.0

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

July 2021 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2007-1562	CVE-2020-35654	CVE-2021-20245	CVE-2021-2381	CVE-2021-25292	CVE-2021-29957
CVE-2019-11750	CVE-2020-36241	CVE-2021-20246	CVE-2021-23839	CVE-2021-25293	CVE-2021-29964
CVE-2019-9792	CVE-2020-36242	CVE-2021-20270	CVE-2021-23840	CVE-2021-26937	CVE-2021-29967
CVE-2020-14150	CVE-2020-8231	CVE-2021-21300	CVE-2021-23841	CVE-2021-27135	CVE-2021-31542
CVE-2020-14343	CVE-2020-8284	CVE-2021-2146	CVE-2021-23961	CVE-2021-27311	CVE-2021-31618
CVE-2020-14387	CVE-2020-8285	CVE-2021-2154	CVE-2021-23991	CVE-2021-27921	CVE-2021-3181
CVE-2020-14409	CVE-2020-8286	CVE-2021-2161	CVE-2021-23992	CVE-2021-27922	CVE-2021-32052
CVE-2020-14410	CVE-2020-9947	CVE-2021-2162	CVE-2021-23993	CVE-2021-27923	CVE-2021-32055
CVE-2020-1747	CVE-2021-1765	CVE-2021-2163	CVE-2021-23994	CVE-2021-28041	CVE-2021-33203
CVE-2020-17525	CVE-2021-1788	CVE-2021-2163	CVE-2021-23995	CVE-2021-28153	CVE-2021-33571
CVE-2020-18032	CVE-2021-1789	CVE-2021-2166	CVE-2021-23998	CVE-2021-28650	CVE-2021-3449
CVE-2020-27918	CVE-2021-1799	CVE-2021-2169	CVE-2021-23999	CVE-2021-28658	CVE-2021-3450
CVE-2020-28493	CVE-2021-1801	CVE-2021-2171	CVE-2021-23999	CVE-2021-28965	CVE-2021-3468
CVE-2020-29599	CVE-2021-1844	CVE-2021-2174	CVE-2021-24002	CVE-2021-29921	CVE-2021-3472
CVE-2020-29623	CVE-2021-1870	CVE-2021-2179	CVE-2021-25214	CVE-2021-29945	CVE-2021-3520
CVE-2020-35492	CVE-2021-1871	CVE-2021-2180	CVE-2021-25215	CVE-2021-29946	CVE-2021-3560
CVE-2020-35521	CVE-2021-20176	CVE-2021-2194	CVE-2021-25216	CVE-2021-29948	

CVE-2020-35522	CVE-2021-20227	CVE-2021-22207	CVE-2021-25289	CVE-2021-29949	
CVE-2020-35523	CVE-2021-20240	CVE-2021-2226	CVE-2021-25290	CVE-2021-29951	
CVE-2020-35524	CVE-2021-20241	CVE-2021-2307	CVE-2021-25311	CVE-2021-29956	

See the US-CERT Common Vulnerability Exposures (CVE) list for Java 7 Update 311 software below:

Java 7 Update 311 Software Remediated US-CERT CVE's			
CVE-2021-2341	CVE-2021-2369	CVE-2021-2432	

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v78.11.0esr software below:

Firefox v78.11.0esr Software Remediated US-CERT CVE's					
CVE-2021-23961	CVE-2021-23995	CVE-2021-23999	CVE-2021-29945	CVE-2021-29951	CVE-2021-29967
CVE-2021-23994	CVE-2021-23998	CVE-2021-24002	CVE-2021-29946	CVE-2021-29964	

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. The FreeFlow® Print Server application supported on Solaris® 11 is not yet supported for install from the Update Manager UI.

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.

1. Xerox® D110/125/136
2. Xerox® Color 800i/1000i Press
3. Xerox® Color 800/1000 Press
4. Xerox® Versant® 3100 Press

This Security patch deliverable has been tested on the FreeFlow® Print Server 93.K4.85.11 software release. The July 2021 Security Patch Cluster is not supported on any earlier FreeFlow® Print Server 9.3 release given a dependency on the Solaris 11.4 OS.

The July 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. Example output from this script for the FreeFlow® Print Server v9 software is as follows:

Solaris® OS Version:	11.4
FFPS Release Version	9.0_SP-3_(93.K4.85.86)
FFPS Patch Cluster	July 2021
Java Version	Java 7 Update 311
Base Repository	Installed
Firefox Version	78.11.0esr
Spectre Variant #1	Installed
Meltdown Variant #3	Installed
Spectre Variant #2	Not Installed

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

July 2021 Security Patch Cluster Files

Security Patch File	Windows® Size (K-bytes)	Solaris® Size (bytes)	Solaris® Checksum
Jul2021AndJava7Update311Patches_v9S11_4-Part1.zip	2,273,149	2,327,704,370	62504 4546298
Jul2021AndJava7Update311Patches_v9S11_4-Part2.zip	3,839,811	3,931,965,922	47232 7679621
Jul2021AndJava7Update311Patches_v9S11_4-Part3.zip	3,671,407	3,759,519,959	7292 7342813
Jul2021AndJava7Update311Patches_v9S11_4-Part4.zip	3,464,217	3,547,357,295	29427 6928433

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 **Jan2021AndJava7Update311Patches_v9S11_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