

# Xerox Security Bulletin XRX24-010

## Xerox® FreeFlow® Print Server v7

**For:** Solaris® 11.4 Operating System

**Install Method:** DVD/USB Media

**Supports:** Xerox Nuvera® PSIP RV 14.5 Printer Products

**Deliverable:** April 2024 Security Patch Cluster

**Includes:** OpenJDK 8 Update 412-b08, Apache HTTP 2.4.59, Apache Tomcat 8.5.96 and Firefox 115.9.0.esr Software

**Bulletin Date:** May 28, 2024

### 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 authorizes 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 2024 Security Patch Cluster

- Supersedes January 2024 Security Patch Cluster
- This Patch Cluster is only intended for FFPS 73.M1.90 / RV 14.4.28 and 73.N2.74 / RV 14.5.34 software releases. If an earlier software release is installed it's recommended to first install the FFPS 73.N2.74 / RV 14.5.34 software release.

#### 2. OpenJDK 8 Update 412-b08 Software

- Supersedes Open JDK 8 Update 392-b07 Software.

#### 3. Apache HTTP 2.4.59 Software

- Supersedes Apache HTTP 2.4.58 Software.

#### 4. Apache Tomcat 8.5.96 Software

#### 5. Firefox 115.9.0.esr Software

- Supersedes Firefox 115.5.0esr Software.

### Caveats:

1. The April 2024 Security Patch Cluster breaks the IP Filtering feature. If you rely on the IP Filtering feature, please submit an escalation to the Xerox hotline to get a fix for this issue.
2. SFTP connection attempts to a Nuvera printer will fail if using weak encryption algorithms. If the SFTP application supports SHA2 hash and AES 512-bit stream encryption strengths connectivity will be successful.

The Xear Flex application is no longer able to connect to the printer using a secure FTP (SFTP) request until updated with stronger encryption algorithms. A customer may refuse to install the April 2024 Security Patch Cluster if it breaks their secure connection for Xear Flex until there is a fix for this issue. A customer would need to determine if Xear Flex or installing the latest Security Patch Cluster is more important to them.

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 412-b08 software below:

**OpenJDK 8 Update 412-b08 Software Remediated US-CERT CVE's**

|                |                |                |                |
|----------------|----------------|----------------|----------------|
| CVE-2024-21011 | CVE-2024-21068 | CVE-2024-21085 | CVE-2024-21094 |
|----------------|----------------|----------------|----------------|

See the US-CERT Common Vulnerability Exposures (CVE) the April 2024 Security Patch Cluster remediate in table below:

**April 2024 Security Patch Cluster Remediated US-CERT CVE's**

|                |                |                |               |                |                |
|----------------|----------------|----------------|---------------|----------------|----------------|
| CVE-2023-50868 | CVE-2023-41175 | CVE-2023-49990 | CVE-2023-5574 | CVE-2024-0209  | CVE-2024-20999 |
| CVE-2014-10401 | CVE-2023-43785 | CVE-2023-49991 | CVE-2023-5679 | CVE-2024-0210  | CVE-2024-21059 |
| CVE-2014-10402 | CVE-2023-43786 | CVE-2023-49992 | CVE-2023-5764 | CVE-2024-0211  | CVE-2024-21105 |
| CVE-2020-22218 | CVE-2023-43787 | CVE-2023-49993 | CVE-2023-5824 | CVE-2024-0727  | CVE-2024-21890 |
| CVE-2020-27545 | CVE-2023-43788 | CVE-2023-49994 | CVE-2023-6174 | CVE-2024-0741  | CVE-2024-21891 |
| CVE-2020-28162 | CVE-2023-43789 | CVE-2023-50387 | CVE-2023-6175 | CVE-2024-0742  | CVE-2024-21896 |
| CVE-2020-28163 | CVE-2023-4408  | CVE-2023-50447 | CVE-2023-6377 | CVE-2024-0743  | CVE-2024-22019 |
| CVE-2022-22817 | CVE-2023-44487 | CVE-2023-50761 | CVE-2023-6478 | CVE-2024-0746  | CVE-2024-22195 |
| CVE-2022-32200 | CVE-2023-45285 | CVE-2023-50762 | CVE-2023-6516 | CVE-2024-0747i | CVE-2024-24680 |
| CVE-2022-34299 | CVE-2023-46728 | CVE-2023-50868 | CVE-2023-6856 | CVE-2024-0749  | CVE-2024-24806 |
| CVE-2022-39170 | CVE-2023-4675  | CVE-2023-51384 | CVE-2023-6857 | CVE-2024-0750  | CVE-2024-25617 |
| CVE-2022-40982 | CVE-2023-46751 | CVE-2023-51385 | CVE-2023-6858 | CVE-2024-0751  | CVE-2024-2605  |
| CVE-2022-46285 | CVE-2023-46809 | CVE-2023-51713 | CVE-2023-6859 | CVE-2024-0753  | CVE-2024-2607  |
| CVE-2022-46344 | CVE-2023-46846 | CVE-2023-51765 | CVE-2023-6860 | CVE-2024-0755  | CVE-2024-2608  |
| CVE-2023-22053 | CVE-2023-46847 | CVE-2023-52355 | CVE-2023-6861 | CVE-2024-1546  | CVE-2024-2610  |
| CVE-2023-27371 | CVE-2023-46848 | CVE-2023-52356 | CVE-2023-6862 | CVE-2024-1547  | CVE-2024-2611  |
| CVE-2023-34872 | CVE-2023-47038 | CVE-2023-5363  | CVE-2023-6863 | CVE-2024-1548  | CVE-2024-2612  |
| CVE-2023-38408 | CVE-2023-47100 | CVE-2023-5367  | CVE-2023-6864 | CVE-2024-1549  | CVE-2024-2614  |
| CVE-2023-39326 | CVE-2023-48795 | CVE-2023-5371  | CVE-2023-6865 | CVE-2024-1550  | CVE-2024-2616  |
| CVE-2023-39615 | CVE-2023-49285 | CVE-2023-5380  | CVE-2023-6867 | CVE-2024-1551  |                |
| CVE-2023-40305 | CVE-2023-49286 | CVE-2023-5388  | CVE-2024-0207 | CVE-2024-1552  |                |
| CVE-2023-40745 | CVE-2023-49288 | CVE-2023-5517  | CVE-2024-0208 | CVE-2024-1553  |                |

See the US-CERT Common Vulnerability Exposures (CVE) list for OpenJDK 8 Update 412-b08 software below:

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache HTTP 2.4.59 software below:

**Apache HTTP 2.4.59 Software Remediated US-CERT CVE's**

|                |                |                |  |
|----------------|----------------|----------------|--|
| CVE-2023-38709 | CVE-2024-27316 | CVE-2024-24795 |  |
|----------------|----------------|----------------|--|

See the US-CERT Common Vulnerability Exposures (CVE) list for Apache Tomcat 8.5.96 software below:

**Apache Tomcat 8.5.96 Software Remediated US-CERT CVE's**

|                |  |  |  |
|----------------|--|--|--|
| CVE-2023-46589 |  |  |  |
|----------------|--|--|--|

See the US-CERT Common Vulnerability Exposures (CVE) list for the Firefox v115.9.0.esr software below:

| Firefox v115.9.0.esr Software Remediated US-CERT CVE's |               |               |               |               |               |
|--------------------------------------------------------|---------------|---------------|---------------|---------------|---------------|
| CVE-2023-5388                                          | CVE-2023-6862 | CVE-2024-0743 | CVE-2024-0755 | CVE-2024-1552 | CVE-2024-2612 |
| CVE-2023-6856                                          | CVE-2023-6863 | CVE-2024-0746 | CVE-2024-1546 | CVE-2024-1553 | CVE-2024-2614 |
| CVE-2023-6857                                          | CVE-2023-6864 | CVE-2024-0747 | CVE-2024-1547 | CVE-2024-2605 | CVE-2024-2616 |
| CVE-2023-6858                                          | CVE-2023-6865 | CVE-2024-0749 | CVE-2024-1548 | CVE-2024-2607 |               |
| CVE-2023-6859                                          | CVE-2023-6867 | CVE-2024-0750 | CVE-2024-1549 | CVE-2024-2608 |               |
| CVE-2023-6860                                          | CVE-2024-0741 | CVE-2024-0751 | CVE-2024-1550 | CVE-2024-2610 |               |
| CVE-2023-6861                                          | CVE-2024-0742 | CVE-2024-0753 | CVE-2024-1551 | CVE-2024-2611 |               |

**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.

## 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 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 2024 Security Patch Cluster is available for the FreeFlow® Print Server 73.N2.74 / RV 14.5.34 software release on the Solaris® 11.4 OS for the Nuvera® 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.N2.74.11 / RV 14.5.34 software release. Although it was not tested with the FreeFlow® Print Server 73.M1.90 / RV 14.4.28 software release, this release is supported, and the installation should be successful.

The April 2024 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, OpenJDK Software version. Example output from this script for the FreeFlow® Print Server v7 software is as follows:

|                             |                           |
|-----------------------------|---------------------------|
| <b>Solaris® OS Version:</b> | 11.4.68.164.2             |
| <b>FFPS Release Version</b> | 7.0_SP-3 (73.N2.74.11.86) |
| <b>FFPS Patch Cluster</b>   | April 2024                |
| <b>Java Version</b>         | OpenJDK 8 Update 412      |

The above versions are the correct information after installing the April 2024 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 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 installation 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 2024 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 installation. Once the patch cluster has been prepared on the hard disk, a script is run to perform the installation. Alternatively, the April 2024 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 patches is corrupted 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 illustrates file size on Windows®, file size on Solaris® and checksum on Solaris® for the April 2024 Security Patch Cluster files.

April 2024 Security Patch Cluster Files

| Security Patch File                                  | Windows®<br>Size (K-<br>bytes) | Solaris®<br>Size (bytes) | Solaris®<br>Checksum |
|------------------------------------------------------|--------------------------------|--------------------------|----------------------|
| Apr2024AndOpenJDK8Update412Patches_v7S11_4-Part1.zip | 3,859,201                      | 3,951,820,923            | 3852 7718401         |
| Apr2024AndOpenJDK8Update412Patches_v7S11_4-Part2.zip | 3,293,427                      | 3,372,469,218            | 41435 6586854        |
| Apr2024AndOpenJDK8Update412Patches_v7S11_4-Part3.zip | 4,890,983                      | 5,008,366,503            | 35128 9781966        |
| Apr2024AndOpenJDK8Update412Patches_v7S11_4-Part4.zip | 4,805,501                      | 4,920,832,343            | 22218 9611001        |

Verify integrity of the Security Patch files from the FreeFlow® Print Server hard drive by comparing the actual checksum (using UNIX ‘sum’ command) of these files copied to the platform with the Solaris checksum in the above table. Change directory to the directory location where the Security Patch Cluster file was copied and use the UNIX ‘sum’ command to output the check sum numbers of each ZIP file (E.g., **sum Apr2024AndOpenJDK8Update412Patches\_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 a 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.

