Xerox Security Bulletin XRX17-029
Xerox® FreeFlow® Print Server 8

Update Manager Delivery of: October 2017 Security Patch Cluster
Includes: Java 6 Update 171
Bulletin Date: December 4, 2017

1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Solaris Operating platform. Oracle® does not provide these patches to the public, but authorize vendors like Xerox® to deliver them to Customers with 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. **October 2017 Security Patch Cluster**
   - This supersedes the July 2017 Security Patch Cluster
2. **Java 6 Update 171 Software**
   - This supersedes Java 6 Update 161 Software

CAVEAT: We have a caveat with the October 2017 Security Patch Cluster for the FFPS 7.3 and 9.3 software releases. The FFPS application is not able to access remote SMB shares after installing the October 2017 Security Patch Cluster. This does not affect the SMB shares used for Hot Folder workflow. The affected capabilities are SMB access of remote job files by the 'Print From File' client, and storing PDF/TIFF files to a remote location over SMB from a hardcopy scan (E.g., commonly done on a Nuvera printer). It is not common for a Security conscience customer to use SMB workflows, so this should not affect many customers.

See US-CERT Common Vulnerability Exposures (CVE) the October 2017 Security Patch Cluster remediate in table below:

October 2017 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2016-1238	CVE-2017-6452	CVE-2017-7186	CVE-2017-8343	CVE-2017-8351	CVE-2017-8779
CVE-2016-9042	CVE-2017-6455	CVE-2017-7244	CVE-2017-8344	CVE-2017-8352	CVE-2017-8786
CVE-2017-11103	CVE-2017-6458	CVE-2017-7245	CVE-2017-8345	CVE-2017-8353	CVE-2017-8804
CVE-2017-3167	CVE-2017-6459	CVE-2017-7246	CVE-2017-8346	CVE-2017-8354	CVE-2017-8830
CVE-2017-3169	CVE-2017-6460	CVE-2017-7619	CVE-2017-8347	CVE-2017-8355	CVE-2017-9098
CVE-2017-3629	CVE-2017-6462	CVE-2017-7659	CVE-2017-8348	CVE-2017-8356	CVE-2017-9788
CVE-2017-5664	CVE-2017-6463	CVE-2017-7668	CVE-2017-8349	CVE-2017-8357	CVE-2017-9789
CVE-2017-6451	CVE-2017-6464	CVE-2017-7679	CVE-2017-8350	CVE-2017-8765	

See the US-CERT Common Vulnerability Exposures (CVE) the Java 6 Update 171 Software remediate in table below:

Java 6 Update 171 Software CVE Remediated US-CERT CVE's					
CVE-2016-10165	CVE-2017-10281	CVE-2017-10295	CVE-2017-10349	CVE-2017-10347	CVE-2017-10357
CVE-2016-9841	CVE-2017-10285	CVE-2017-10345	CVE-2017-10350	CVE-2017-10348	CVE-2017-10388
CVE-2017-10274	CVE-2017-10293	CVE-2017-10346	CVE-2017-10355	CVE-2017-10356	

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

Xerox offers the Security Patch Update delivery available over the network from a Xerox server using an application called FreeFlow® Print Server Update Manager. The use of FreeFlow® Print Server Update Manager (GUI-based application) makes it simple for a customer to install Security patch updates.

The FreeFlow® Print Server Update Manager delivery of the Security Patch Cluster provides the ability to install Security patches on top of a pre-installed FreeFlow® Print Server software release. The advantage of this network install method is the "ease of deliver and install" of this network delivery from a Xerox patch server over the Internet. This easy install method give a FreeFlow® Print Server customer the option to manage the quarterly Security Patch Cluster install without need for support from Xerox service. This empowers the customer to have the option of installing these patch updates as soon as they become available, and not need to rely on the Xerox Service team. Many customers do not want the responsibility of installing the quarterly Security Patch Update or they are not comfortable providing a network tunnel to the Xerox or Microsoft® servers that store the Security Patch Update. In this case, the media install method (i.e., USB/DVD) is the best option under those circumstances.

A tool is available that enables identification of the currently installed FreeFlow® Print Server software release, Security Patch Cluster, and Java Software version. Run this tool after the Security Patch Cluster install to validate successful install. Example output from this script for the FreeFlow® Print Server v8 software release is as following:

FFPS Release Version	8.0-2_SP-2_(81.G3.03.86)
FFPS Patch Cluster	October 2017
Java Version	Java 6 Update 171

The October 2017 Security Patch Cluster is available for the FreeFlow® Print Server Software Releases below:

FreeFlow® Print Server v8

Xerox® printer products running the FreeFlow® Print Server 81.G3.03 software release for:

- Xerox® iGen®4 Press
- Xerox® Color 800/1000 Press
- Xerox® Color 560/570 Printer
- Xerox ® 700/700i Digital Color Press
- Xerox ® 770 Digital Color Press

All previous FreeFlow® Print Server v8.2 software releases have not been tested with October 2017 Security Patch Cluster, but there should not be any problems on previous FreeFlow® Print Server 8.2 releases.

3.0 Patch Install

Xerox® strives to deliver Security Patch Clusters 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, or use Update Manager to install as the System Administrator. Update Manager is a GUI tool on the FreeFlow® Print Server platform used to check for Security patches, download Security patches, and install Security patches. The customer can install a quarterly Security Patch Cluster using the Update Manager UI, or schedule Xerox Service to perform the install.

Once the Security patches are ready for customer delivery, they are available from the Xerox patch server. Procedures are available for the FreeFlow® Print Server System Administrator or Xerox Service for using the Update Manager GUI to download and install the Security patches over the Internet. The Update Manager UI has a '**Check for Updates**' button that can be selected to retrieve and list patch updates available from the Xerox patch server. When this option is selected the latest Security Patch Cluster should be listed (E.g., **October 2017 Security Patch Cluster for FFPS v8.2**) as available for download and install. The Update Manager UI includes mouse selectable buttons to download and then install the patches.

Xerox® uploads the Security Patch Cluster to a Xerox patch server that is available on the Internet outside of the Xerox Corporate network once the deliverable has been tested and approved. Once in place on the Xerox server, a CSE/Analyst or the customer can use FreeFlow® Print Server Update Manager UI to download and install on the FreeFlow® Print Server platform.

The customer proxy information is required to be setup on the FreeFlow® Print Server platform so it can access to the Security Patch Update over the Internet. The FreeFlow® Print Server platform initiates a "secure" communication session with the Xerox patch server using HTTP over the TSL 1.2 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, and SHA1 encryption. This connection ensures authentication of the FreeFlow® Print Server platform for the Xerox server, and sets up encrypted communication of the patch data. The Xerox server does not initiate or have access to the FreeFlow® Print Server platform behind the customer firewall. The Xerox server and FreeFlow® Print Server platform both authenticate each other before making a connection between the two end-points, and patch data transfer.

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.