Xerox Security Bulletin XRX17-020

Xerox® FreeFlow® Print Server v8

Update Manager Network Delivery of:
July 2017 Security Patch Cluster
Java 6 Update 161

Bulletin Date: August 10, 2017

A. 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. **July 2017 Security Patch Cluster**
   - This supersedes the April 2017 Security Patch Cluster
2. **Java 6 Update 161 Software**
   - This supersedes Java 6 Update 151 Software

See the US-CERT Common Vulnerability Exposures (CVE's) remediated by the July 2017 Security Patch Cluster illustrated below:

July 2017 Security Patch Cluster CVE Remediation Table					
CVE-2013-7447	CVE-2015-8875	CVE-2017-10003	CVE-2017-10036	CVE-2017-2619	CVE-2017-3630
CVE-2014-9766	CVE-2016-10164	CVE-2017-10004	CVE-2017-10042	CVE-2017-3622	CVE-2017-3632
CVE-2015-7674	CVE-2016-5384	CVE-2017-10122	CVE-2017-10062	CVE-2017-3629	CVE-2017-7494

See the US-CERT Common Vulnerability Exposures (CVE's) remediated by the Java 6 Update 161 illustrated below:

July 2017 Security Patch Cluster CVE Remediation Table				
CVE-2017-10053	CVE-2017-10089	CVE-2017-10102	CVE-2017-10109	CVE-2017-10135
CVE-2017-10067	CVE-2017-10087	CVE-2017-10105	CVE-2017-10110	CVE-2017-10193
CVE-2017-10074	CVE-2017-10096	CVE-2017-10107	CVE-2017-10115	CVE-2017-10198
CVE-2017-10081	CVE-2017-10101	CVE-2017-10108	CVE-2017-10116	CVE-2017-10243

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.

B. 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 Oracle 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 FFPS 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	July 2017
Java Version	Java 6 Update 161

The July 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:

1. Xerox® iGen®4 Press
2. Xerox® Color 560/570 Printer
3. Xerox ® 700i/700 Digital Color Press

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

C. Patch Install

Xerox strives to deliver Security Patch Clusters in a timely manner. The customer process to obtain FFPS Security Patch Cluster updates (delivered on a quarterly basis) is to contact the Xerox hotline support number, or use FFPS Update Manager to install as the System Administrator. FFPS Update Manager is a GUI tool on the FFPS platform used to check for Security patches, download Security patches, and install Security patches. The customer can install a quarterly FFPS Security Patch Cluster using the FFPS 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 FFPS 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 FFPS Security Patch Cluster should be listed (E.g., "July 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 FFPS platform so it can access to the Xerox patch over the Internet. The FFPS platform initiates a "secure" communication session with the Xerox patch server using HTTP over the SSLv3 protocol (HTTPS on port 443) using a VeriSign certificate. This connection ensures authentication of the FFPS 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 FFPS platform behind the customer firewall. The Xerox server and FFPS system both authenticate each other before making a connection between the two end-points, and patch data transfer.

The customer proxy information is required to be setup on the FFPS platform so it can access to the Security Patch Update over the Internet. The FFPS 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 FFPS 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 FFPS platform behind the customer firewall. The Xerox server and FFPS system both authenticate each other before making a connection between the two end-points, and patch data transfer.

D. 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.