Xerox Security Bulletin XRX17-005

Xerox® FreeFlow® Print Server v7 and v9
Update Manager Network Delivery of:
January 2017 Security Patch Cluster
Java 7 Update 121

Bulletin Date: March 6, 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. **January 2017 Security Patch Cluster**
   - This supersedes the October 2016 Security Patch Cluster
2. **Java 7 Update 121 Software**
   - Same as included with the October 2016 Security Patch Cluster
   - This supersedes Java 7 Update 111 Software

Remediated US-CERT Security Common Vulnerability Exposures (CVE's)					
CVE-2015-3228	CVE-2016-2335	CVE-2016-6302	CVE-2016-7101	CVE-2016-7522	CVE-2016-7532
CVE-2015-8957	CVE-2016-3465	CVE-2016-6303	CVE-2016-7513	CVE-2016-7523	CVE-2016-7533
CVE-2015-8958	CVE-2016-5384	CVE-2016-6304	CVE-2016-7514	CVE-2016-7524	CVE-2016-7534
CVE-2016-2177	CVE-2016-5542	CVE-2016-6305	CVE-2016-7515	CVE-2016-7525	CVE-2016-7535
CVE-2016-2178	CVE-2016-5554	CVE-2016-6306	CVE-2016-7516	CVE-2016-7526	CVE-2016-7536
CVE-2016-2179	CVE-2016-5556	CVE-2016-6307	CVE-2016-7517	CVE-2016-7527	CVE-2016-7537
CVE-2016-2180	CVE-2016-5568	CVE-2016-6308	CVE-2016-7518	CVE-2016-7528	CVE-2016-7538
CVE-2016-2181	CVE-2016-5573	CVE-2016-6309	CVE-2016-7519	CVE-2016-7529	CVE-2016-7539
CVE-2016-2182	CVE-2016-5582	CVE-2016-6823	CVE-2016-7520	CVE-2016-7530	CVE-2016-7540
CVE-2016-2183	CVE-2016-5597	CVE-2016-7052	CVE-2016-7521	CVE-2016-7531	CVE-2016-8864

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 a 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 v9 software release is as following:

FFPS Release Version	9.0_SP-3 (93.G3.74A)
FFPS Patch Cluster	January 2017
Java Version	Java 7 Update 121

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

FreeFlow® Print Server v7

Xerox printer products running the FreeFlow® Print Server 73.G2.55 software release for:

1. Xerox Nuvera® 100/120/144/157 EA Digital Production System
2. Xerox Nuvera® 200/288/314 EA Perfecting Production System
3. Xerox Nuvera® 100/120/144 MX Digital Production System
4. Xerox Nuvera® 200/288 MX Perfecting Production System
5. Xerox® DocuPrint 100/115/135/155/180 MX Enterprise Printing System
6. Xerox® DocuTech® 6128/6155/6180 Production Publisher
7. Xerox® DocuTech® Highlight Color 128/155/180 Production Publisher
8. Xerox® DocuColor® 242/252/260/700,
9. Xerox® DocuColor® 5000AP
10. Xerox® DocuColor® 7002/8002
11. Xerox® DocuColor® 8080
12. Xerox® Digital Printer 4112/4127 Enterprise Printing System
13. Xerox® Digital 4590/4595 Copier/Printer

All previous FreeFlow® Print Server v7.3 software releases have not been tested with January 2017 Security Patch Cluster, but there should not be any problems on previous FreeFlow® Print Server 7.3 releases.

FreeFlow® Print Server v9

Xerox printer products running the FreeFlow® Print Server 93.G4.74A software release for:

1. Xerox® iGen® Products (iGen4, iGen150, Xerox® Color 8250 Presses)
2. Xerox® Versant 80/2100 Presses
3. Xerox® Color 800/100, 800i/1000i Presses
4. Xerox® Color Press J75/C75 Presses
5. Xerox® Color Press 560/570
6. Xerox® Impika® Compact Inkjet Press
7. Xerox® CiPress® 325/500 Production Inkjet System
8. Xerox® Rialto® 900 Inkjet Press
9. Xerox® D95/110/125/136 Copier/Printers

All previous FreeFlow® Print Server v9.3 software releases have not been tested with January 2017 Security Patch Cluster, but there should not be any problems on previous FreeFlow® Print Server 9.3 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., "January 2017 Security Patch Cluster for FFPS v9.3") 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.