Xerox Security Bulletin XRX18-004

Xerox® FreeFlow® Print Server v7 and v9

Update Manager Delivery of: January 2018 Security Patch Cluster
Includes: Java 7 Update 171
Bulletin Date: February 10, 2018

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. **January 2018 Security Patch Cluster**
   - This supersedes the October 2017 Security Patch Cluster
2. **Java 7 Update 171 Software**
   - This supersedes Java 7 Update 161 Software

CAVEAT: We have a caveat with the January 2018 Security Patch Cluster for the FreeFlow® Print Server 7.3 and 9.3 software releases. The FreeFlow Print Server application is not able to access remote SMB shares after installing the January 2018 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 January 2018 Security Patch Cluster remediate in table below:

January 2018 Security Patch Cluster Remediated US-CERT CVE's					
CVE-2011-2391	CVE-2016-0701	CVE-2017-1000083	CVE-2017-12163	CVE-2017-3736	CVE-2018-2710
CVE-2015-3193	CVE-2016-5824	CVE-2017-12150	CVE-2017-14989	CVE-2017-3737	
CVE-2015-7674	CVE-2016-9584	CVE-2017-12151	CVE-2017-3732	CVE-2017-3738	

See the US-CERT Common Vulnerability Exposures (CVE) the Java 7 Update 171 Software remediate in table below:

Java 7 Update 171 Software Remediated US-CERT CVE's					
CVE-2018-2579	CVE-2018-2599	CVE-2018-2618	CVE-2018-2634	CVE-2018-2657	CVE-2018-2678
CVE-2018-2581	CVE-2018-2602	CVE-2018-2629	CVE-2018-2637	CVE-2018-2663	
CVE-2018-2588	CVE-2018-2603	CVE-2018-2633	CVE-2018-2641	CVE-2018-2677	

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 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" from a Xerox patch server over the Internet. This easy install method gives a FreeFlow® Print Server customer the option to manage quarterly Security Patch Cluster install without need for support from Xerox service. This empowers the customer to have the option of installing 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® Xerox® communication server that stores Security patches. In this case, the media install method (i.e., USB/DVD) is the best option under those circumstances.

This Security patch deliverable has been tested on the FreeFlow® Print Server 73.H3.72, 93.H2.23A and 93.10.04A software releases. We have not tested the January 2018 Security Patch Cluster on all earlier FreeFlow® Print Server 7.3 and 9.3 releases, but there should not be any problems on these releases.

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 v7 software release is as following:

FFPS Release Version	7.0_SP-3_(73.H3.72.86)
FFPS Patch Cluster	January 2018
Java Version	Java 7 Update 171

The January 2018 Security Patch Cluster is available for the FreeFlow® Print Server v7 release running on the Xerox® printer products below:

1. Xerox Nuvera® 100/120 Digital Coper/Printer
2. Xerox Nuvera® 100/120/144 Digital Production System
3. Xerox Nuvera® 100/120/144/157 EA Digital Production System
4. Xerox Nuvera® 200/288/314 EA Perfecting Production System
5. Xerox Nuvera® 100/120/144 MX Digital Production System
6. Xerox Nuvera® 200/288 MX Perfecting Production System
7. Xerox® DocuPrint® 100/115/135/155/180 MX Enterprise Printing System
8. Xerox® DocuTech® 6128/6155/6180 Production Publisher
9. Xerox® DocuTech® 128/155/180 Highlight Color Production Publisher
10. Xerox® DocuColor® 242/252/260 Digital Color Printer/Copiers
11. Xerox® DocuColor® 5000AP/7000AP/8000AP Digital Press
12. Xerox® DocuColor® 7000/7002/8000/8002/8080 Presses
13. Xerox® Digital Printer 4112/4127 Enterprise Printing System
14. Xerox® Digital 4590/4595 Copier/Printer
15. Xerox® Color 8250 Production Press

The January 2018 Security Patch Cluster is available for the FreeFlow® Print Server v9 release running on the Xerox® printer products below:

1. Xerox® iGen®4
2. Xerox® iGen®4 Diamond Edition®
3. Xerox® iGen®150 Press
4. Xerox® Versant® 80/180/2100 Presses

5. Xerox® Color 800/100 Presses
6. Xerox® Color 800i/1000i Presses
7. Xerox® Color Press J75/C75 Presses
8. Xerox® Color Press 560/570 Production Printer
9. Xerox® Brenva® HD Production Inkjet Press
10. Xerox® Impika® Compact Inkjet Press
11. Xerox® CiPress® 325/500 Production Inkjet System
12. Xerox® D95/110/125/136 Copier/Printer

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. The Update Manager is a GUI tool on the FreeFlow® Print Server platform used to check for Security patches, download 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 communication server. Procedures are available for the Customer 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 communication server. When this option is selected the latest Security Patch Cluster should be listed (E.g., **January 2018 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 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 communication server using HTTP over the TLS 1.0 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, SHA2 hash and AES 256-bit stream encryption algorithms. 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.