Xerox Security Bulletin XRX16-003 V1.0

FreeFlow Print Server v7, v8 and v9
Update Manager Network Delivery of:
- October 2015 Security Patch Cluster (includes Java 6 Update 105)

01/13/2016

Background

Oracle delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Solaris Operating System. Oracle does not provide these patches to the general public, but Xerox is authorized to deliver them to Customers with active FreeFlow Print Server (FFPS) Support Contracts (FSMA). Customers who may have an Oracle Support Contract for their non-FFPS Solaris Servers should not install patches that have not been customized by Xerox. Otherwise the FFPS software could be damaged and result in downtime and a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **October 2015 Security Patch Cluster**
   - ✓ This supersedes the July 2015 Security Patch Cluster
2. **Java 6 Update 105 Software**
   - ✓ This supersedes Java 6 Update 101 Software

The Security vulnerabilities that are remediated with this FFPS Security patch delivery are as follows:

CVE-2008-4770	CVE-2009-0696	CVE-2014-7185	CVE-2015-2642	CVE-2015-4734	CVE-2015-4803
CVE-2015-4805	CVE-2015-4806	CVE-2015-4835	CVE-2015-4842	CVE-2015-4843	CVE-2015-4844
CVE-2015-4860	CVE-2015-4869	CVE-2015-4872	CVE-2015-4881	CVE-2015-4882	CVE-2015-4883
CVE-2015-4893	CVE-2015-4902	CVE-2015-4903	CVE-2015-4911		

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 FFPS DFE.

Applicability

The Xerox Customer Service Engineer (CSE)/Analyst is provided a tool (accessible from CFO Web site) that enables the analyst to confirm the currently installed FFPS software release, Security Patch Cluster, and Java Software version. When this Security update has been installed on the FFPS system, example output from this script for the FFPS v8 software release is as following:

FFPS Release Version: 8.0_SP-2 (82.E2.34)
FFPS Patch Cluster: October 2015
Java Version: Java 6 Update 105

Patch Install

Xerox strives to deliver Security patch updates 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 DFE that can be used to "check for Security updates", download Security updates, and install Security updates. The customer can install quarterly FFPS Security Patch Clusters 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 made available from the Xerox Edge Host and Download servers. 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 list patch updates available from the Xerox Edge Host server. When this option is selected the latest FFPS Security Patch Cluster should be listed (e.g., "October 2015 Security Patch Cluster (FFPS v9.3)") as available for download and install.

This requires that the FFPS system be configured with the customer proxy information to gain Security patch update access from the Xerox servers. The connection is initiated by the FFPS system and the Xerox servers do not have access to the customer network. The Xerox server and FFPS system both authenticate each other before a data transfer can be successfully established between the two end points.

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.