Xerox Security Bulletin XRX12-010

FreeFlow Print Server v8

July 2012 Security Patch Cluster (includes Java 6 Update 33 Software)
V1.1
10/19/2012

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 no longer provides 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. July 2012 Security Patch Cluster
   - ✓ This supersedes the April 2012 Security Patch Cluster
2. Java 6 Update 33 Software
   - ✓ This supersedes Java 6 Update 31 Software

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

CVE-2004-0981
CVE-2005-0759
CVE-2005-0760
CVE-2005-0761
CVE-2005-0762
CVE-2005-1739
CVE-2006-7250
CVE-2007-4985
CVE-2007-4986
CVE-2007-4987
CVE-2007-4988
CVE-2008-3529
CVE-2010-4008
CVE-2011-1944
CVE-2011-2699
CVE-2011-3607
CVE-2011-4028
CVE-2011-4317
CVE-2011-4516
CVE-2011-4517
CVE-2012-0031
CVE-2012-0053
CVE-2012-0563
CVE-2012-0768
CVE-2012-0769
CVE-2012-1173
CVE-2012-1182
CVE-2012-1750
CVE-2012-1765
CVE-2012-2110
CVE-2012-2131
CVE-2012-2333
CVE-2012-3112
CVE-2012-3121
CVE-2012-3123
CVE-2012-3124
CVE-2012-3127
CVE-2012-3129
CVE-2012-3131
CVE-2012-0551
CVE-2012-1711
CVE-2012-1713
CVE-2012-1716
CVE-2012-1717
CVE-2012-1718
CVE-2012-1719
CVE-2012-1720
CVE-2012-1721
CVE-2012-1722
CVE-2012-1723
CVE-2012-1724
CVE-2012-1725

For more details on the vulnerabilities shown in the table above, you can go to the US CERT web site: http://www.us-cert.gov/

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.

Applicability

The FFPS 82.C3.31 (for EPC), 82.C3.31 (for XC 550/560) and 81.C2.03 (for iGen4) software releases are the latest supported for this FFPS Security Patch Cluster delivery. The July 2012 Security Patch Cluster has not been tested with the FFPS 81.B0.34A and 82.C1.41 software releases, but there should not be any problem on these releases.

The Xerox CSE/Analyst is provided a tool (accessible from CFO Web site) that enables them 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, this script will output the following:

FFPS Release Version:	8.0_SP-2 (82.C1.41.86)
FFPS Patch Cluster:	July 2012
Java Version:	Java 6 Update 33

Patch Install Methods

The install of these Security patches must be performed by the Xerox Customer Service Engineer (CSE) or Analyst. The customer process to obtain this Security update is to call the Xerox support number to request the service.

Xerox strives to deliver these critical Security patch updates in a timely manner. They are available from the Xerox Support organization, and can be delivered electronically over the Internet to the FFPS system via a GUI tool called the FFPS Update Manager. The other method of delivery is an FTP transfer to the FFPS system or writing the patch cluster to DVD/USB media. A more detailed description of the methods used by the CSE/Analyst to install the Security patches is as follows:

FFPS Update Manager GUI

Once the Security patches are ready for customer delivery they are made available from the Xerox Edge Host and Download servers. The CSE/Analyst uses the Update Manager GUI on the FFPS system to download and install the Security patches over the Internet. When the Xerox server is checked for updates from FFPS Update Manager, this Security patch update is listed as "**July 2012 Security Patch Cluster (FFPS v8)**".

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.

Hard Disk, DVD/USB Media

Once the Security patch updates are ready for customer delivery they are made available on the CFO Web site. The CSE/Analyst can download and prepare for the install by writing the Security patch update into a well-known directory on the FFPS system, or on DVD/USB media. The FFPS Security Patch Cluster is delivered as an ISO image and ZIP archive file to provide the Xerox Service Representative options to choose an install method. Once the patch cluster has been prepared on media an install script can be run to perform the install. The install script accepts an argument that identifies the media that contains a copy of the FFPS Security Patch Cluster. (E.g., # installSecPatches.sh [disk | dvd | usb]).

Important: *The install of this Security patch update can fail if the archive file containing the patches is corrupted from file transfer or writing to DVD media. There have been reported install failures when the archive file written on DVD media was corrupt. The Security patch update could be corrupted when writing to media by particular DVD burn applications writing on some DVD media types. It is very important that the Security patch archive written onto the DVD install media be verified with the original archive file that was written to DVD.*

The Security patch cluster is delivered as a ZIP and an ISO file. The file size and check sum of these files on Windows and Solaris are as follows:

Security Patch File	Windows Size (Kb)	Solaris Size (bytes)	Solaris Checksum
July2012AndJava6U33Patches_v8.zip	1,595,705	1634361344	26810 3191409
July2012AndJava6U33Patches_v8.iso	1,596,056	1634001366	52424 3192112

*The **July2012AndJava6U33Patches_v8.zip** listed on the DVD media can be verified by comparing it to the original archive file size and checksum. Copy this archive to a location on the FFPS system and type '**sum July2012AndJava6U33Patches_v8.zip**' from a terminal window. The checksum value should be '**26810 3191409'**, and this validates the correct July 2012 Security Patch Cluster is written on the DVD.*

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.