Xerox Security Bulletin XRX13-003

FreeFlow Print Server v8
January 2013 Security Patch Cluster (includes Java 6 Update 37 Software)
v1.0
2/26/2013

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. January 2013 Security Patch Cluster
   - ✓ This supersedes the October 2012 Security Patch Cluster
2. Java 6 Update 37 Software
   - ✓ This supersedes Java 6 Update 33 Software

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

CVE-2006-4514	CVE-2012-0841	CVE-2012-2983	CVE-2012-3968	CVE-2013-0415	CVE-2012-5075
CVE-2008-6536	CVE-2012-0883	CVE-2012-3401	CVE-2012-3969	CVE-2012-1531	CVE-2012-5077
CVE-2011-2697	CVE-2012-1960	CVE-2012-3956	CVE-2012-3970	CVE-2012-1532	CVE-2012-5079
CVE-2011-2964	CVE-2012-1970	CVE-2012-3957	CVE-2012-3972	CVE-2012-1533	CVE-2012-5081
CVE-2011-3102	CVE-2012-1971	CVE-2012-3958	CVE-2012-3974	CVE-2012-3143	CVE-2012-5083
CVE-2011-4339	CVE-2012-1972	CVE-2012-3959	CVE-2012-3976	CVE-2012-3159	CVE-2012-5084
CVE-2012-0569	CVE-2012-1973	CVE-2012-3960	CVE-2012-3978	CVE-2012-3216	CVE-2012-5085
CVE-2012-0724	CVE-2012-1974	CVE-2012-3961	CVE-2012-3980	CVE-2012-4416	CVE-2012-5086
CVE-2012-0725	CVE-2012-1975	CVE-2012-3962	CVE-2012-4245	CVE-2012-5068	CVE-2012-5089
CVE-2012-0768	CVE-2012-1976	CVE-2012-3963	CVE-2012-5166	CVE-2012-5069	
CVE-2012-0769	CVE-2012-2687	CVE-2012-3964	CVE-2013-0399	CVE-2012-5071	
CVE-2012-0772	CVE-2012-2981	CVE-2012-3966	CVE-2013-0400	CVE-2012-5072	
CVE-2012-0773	CVE-2012-2982	CVE-2012-3967	CVE-2013-0407	CVE-2012-5073	

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

These Security updates are intended for Xerox printer products running one of the FFPS 73.C0.41 or 73.B3.61 SPAR software releases. This Security patch update has only been tested on these software releases and it is recommended that they be installed on these FFPS software release versions. They have not been tested with the FFPS 73.B0.73 and 73.A3.31 software 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-3 (82.C5.24.86)
FFPS Patch Cluster: January 2013
Java Version: Java 6 Update 37

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 "**January 2013 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
Jan2013AndJava6U37Patches_v8.zip	1,663,512	1,703,435,583	54151 3327023
Jan2013AndJava6U37Patches_v8.iso	1,615,862	1,703,794,688	13849 3327724

*The **Jan2013AndJava6U37Patches_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 Jan2013AndJava6U37Patches_v8.zip**' from a terminal window. The checksum value should be '**54151 3327023**', and this validates the correct January 2013 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.