Xerox Security Bulletin XRX12-006

FreeFlow Print Server
April 2012 Security Patch Cluster (includes Java 6 Update 31 Software)
v1.0
07/02/2012

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. **April 2012 Security Patch Cluster**
   - ✓ This supersedes the January 2012 Security Patch Cluster
2. **Java 6 Update 31 Software**
   - ✓ This supersedes Java 6 Update 29 Software

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

CVE-2011-4317	**CVE-2012-1683**	**CVE-2011-3232**	**CVE-2007-4826**	**CVE-2012-0497**	**CVE-2012-0505**
CVE-2012-0053	**CVE-2012-1694**	**CVE-2011-3648**	**CVE-2009-1572**	**CVE-2012-0500**	**CVE-2012-0506**
CVE-2011-3368	**CVE-2011-2372**	**CVE-2011-3650**	**CVE-2010-1674**	**CVE-2012-0504**	**CVE-2012-0507**
CVE-2011-3607	**CVE-2011-2995**	**CVE-2011-3650**	**CVE-2010-1675**	**CVE-2012-0497**	**CVE-2011-3563**
CVE-2012-0031	**CVE-2011-2997**	**CVE-2011-3651**	**CVE-2010-2948**	**CVE-2012-0498**	**CVE-2011-5035**
CVE-2012-1681	**CVE-2011-3000**	**CVE-2011-3652**	**CVE-2010-2949**	**CVE-2012-0499**	
CVE-2006-7250	**CVE-2011-3001**	**CVE-2011-3654**	**CVE-2011-3323**	**CVE-2012-0500**	
CVE-2012-1684	**CVE-2011-3002**	**CVE-2011-3655**	**CVE-2011-3324**	**CVE-2012-0501**	
CVE-2011-2728	**CVE-2011-3003**	**CVE-2011-2895**	**CVE-2011-3325**	**CVE-2012-0502**	
CVE-2012-1692	**CVE-2011-3004**	**CVE-2011-4028**	**CVE-2011-3326**	**CVE-2012-0503**	
CVE-2012-0539	**CVE-2011-3005**	**CVE-2011-0465**	**CVE-2011-5035**	**CVE-2012-0504**	

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 the Critical Patch Updates.

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: 7.0_SP-3 (73.C0.41.86)
FFPS Patch Cluster: April 2012
Java Version: Java 6 Update 31

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 from DVD/USB media. A more detailed description of the methods used by the CSE/Analyst to install the Security patches are 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 "**April 2012 Security Patch Cluster (FFPS v7.3)".**

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.

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 write the Security patch update on DVD/USB media. The will need access to either the DVD or USB device on the FFPS platform to install these Security patch updates.

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 archive name is **April2012AndJava6U29Patches_v73.zip**, and the archive written on DVD media can be verified against the original archive by the file size and/or check sum. The file size of the Security patch archive file as viewed from Windows Explorer is '**1,549,414 Kb**' and from a Solaris terminal window is '**1,586,599,791 bytes**'. The check sum can be obtained from a terminal window on the FFPS system by typing '**sum April2012AndJava6U29Patches_v73.zip**'. The check sum output should be '**53289 3098828**'.*

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.