May 23, 2016

Xerox Security Bulletin XRX16-009

FreeFlow Print Server v7, v8 and v9

Update Manager Network Delivery of:

- April 2016 Security Patch Cluster
- Java 6 Update 111 (FFPS v8, v9)
- Java 7 Update 95 (FFPS v7)

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 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 2016 Security Patch Cluster
   - ✓ This supersedes the January 2016 Security Patch Cluster
2. Java 6 Update 115 Software (FFPS V9 & V8)
   - ✓ This supersedes Java 6 Update 111 Software
3. Java 7 Update 101 Software (FFPS V7)
   - ✓ This supersedes Java 7 Update 95 Software

This patch deliverable remediates the US-CERT announced Security vulnerabilities below:

CVE-2004-0548	CVE-2014-8101	CVE-2015-5600	CVE-2015-7871	CVE-2016-0466	CVE-2016-1286
CVE-2012-2814	CVE-2014-8102	CVE-2015-5602	CVE-2015-7973	CVE-2016-0483	CVE-2016-2110
CVE-2014-3566	CVE-2014-8103	CVE-2015-7236	CVE-2015-7974	CVE-2016-0494	CVE-2016-2111
CVE-2014-6271	CVE-2015-0005	CVE-2015-7691	CVE-2015-7975	CVE-2016-0535	CVE-2016-2112
CVE-2014-6277	CVE-2015-0293	CVE-2015-7692	CVE-2015-7976	CVE-2016-0676	CVE-2016-2113
CVE-2014-6278	CVE-2015-3194	CVE-2015-7701	CVE-2015-7977	CVE-2016-0693	CVE-2016-2115
CVE-2014-7169	CVE-2015-3195	CVE-2015-7702	CVE-2015-7978	CVE-2016-0695	CVE-2016-2118
CVE-2014-7186	CVE-2015-3197	CVE-2015-7703	CVE-2015-7979	CVE-2016-0702	CVE-2016-3419
CVE-2014-8091	CVE-2015-3418	CVE-2015-7704	CVE-2015-7981	CVE-2016-0703	CVE-2016-3441
CVE-2014-8092	CVE-2015-4000	CVE-2015-7705	CVE-2015-8126	CVE-2016-0704	CVE-2016-3443
CVE-2014-8093	CVE-2015-5146	CVE-2015-7848	CVE-2015-8138	CVE-2016-0705	CVE-2016-0687
CVE-2014-8094	CVE-2015-5174	CVE-2015-7849	CVE-2015-8139	CVE-2016-0706	CVE-2016-0686
CVE-2014-8095	CVE-2015-5252	CVE-2015-7850	CVE-2015-8140	CVE-2016-0714	CVE-2016-3427
CVE-2014-8096	CVE-2015-5296	CVE-2015-7851	CVE-2015-8158	CVE-2016-0797	CVE-2016-3449
CVE-2014-8097	CVE-2015-5299	CVE-2015-7852	CVE-2015-8472	CVE-2016-0798	CVE-2016-3422
CVE-2014-8098	CVE-2015-5300	CVE-2015-7853	CVE-2015-8704	CVE-2016-0799	CVE-2016-3425
CVE-2014-8099	CVE-2015-5345	CVE-2015-7854	CVE-2016-0402	CVE-2016-0800	CVE-2016-3426
CVE-2014-8100	CVE-2015-5370	CVE-2015-7855	CVE-2016-0448	CVE-2016-1285	

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:	9.0_SP-3 (93.F3.12C)
FFPS Patch Cluster:	April 2016
Java Version:	Java 6 Update 115

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 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., “April 2016 Security Patch Cluster for 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