November 21, 2016

Xerox Security Bulletin XRX16-028

FreeFlow Print Server v7, v8 and v9

Update Manager Network Delivery of:

- October 2016 Security Patch Cluster
- Java 6 Update 131 (FFPS v8)
- Java 7 Update 121 (FFPS v7, v9)

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 2016 Security Patch Cluster**
   - ✓ This supersedes the July 2016 Security Patch Cluster
2. **Java 6 Update 131 Software (v8)**
   - ✓ This supersedes Java 6 Update 121 Software
3. **Java 7 Update 121 Software (v7, v9)**
   - ✓ This supersedes Java 7 Update 111 Software

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

CVE-2012-0876	CVE-2015-1547	CVE-2016-1836	CVE-2016-2518	CVE-2016-4483	CVE-2016-5542
CVE-2012-4564	CVE-2015-5296	CVE-2016-1837	CVE-2016-2519	CVE-2016-4562	CVE-2016-5554
CVE-2013-1619	CVE-2015-5370	CVE-2016-1838	CVE-2016-2775	CVE-2016-4563	CVE-2016-5556
CVE-2013-1960	CVE-2015-7704	CVE-2016-1839	CVE-2016-3189	CVE-2016-4564	CVE-2016-5559
CVE-2013-1961	CVE-2015-8138	CVE-2016-1840	CVE-2016-3627	CVE-2016-4953	CVE-2016-5568
CVE-2013-2116	CVE-2015-8806	CVE-2016-2073	CVE-2016-3705	CVE-2016-4954	CVE-2016-5573
CVE-2013-4231	CVE-2016-0718	CVE-2016-2110	CVE-2016-3714	CVE-2016-4955	CVE-2016-5582
CVE-2013-4232	CVE-2016-1547	CVE-2016-2111	CVE-2016-3715	CVE-2016-4956	CVE-2016-5597
CVE-2013-4243	CVE-2016-1548	CVE-2016-2112	CVE-2016-3716	CVE-2016-4957	CVE-2016-5841
CVE-2013-4244	CVE-2016-1549	CVE-2016-2113	CVE-2016-3717	CVE-2016-4971	CVE-2016-5842
CVE-2014-9330	CVE-2016-1550	CVE-2016-2115	CVE-2016-3718	CVE-2016-5118	CVE-2016-6185
CVE-2014-9655	CVE-2016-1551	CVE-2016-2118	CVE-2016-4447	CVE-2016-5300	CVE-2016-6302
CVE-2015-0005	CVE-2016-1833	CVE-2016-2516	CVE-2016-4448	CVE-2016-5480	CVE-2016-6491
CVE-2015-1283	CVE-2016-1835	CVE-2016-2517	CVE-2016-4449	CVE-2016-5553	

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 Platform.

November 21, 2016

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.G0.85A)
FFPS Patch Cluster:	October 2016
Java Version:	Java 6 Update 131

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., "October 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