Xerox Security Bulletin XRX14-007

FreeFlow Print Server v6, v7, v8 and v9
DocuSP Print Server v5
Bash/Shellshock Security Patch
v1.0
11/06/2014

Background

Oracle has delivered a patch to address US-CERT-announced Security vulnerabilities in the "bash" shell component included in all previously-issued Solaris 10 Operating System Releases. 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. **Bash Security Patch**
   - ✓ This patch has no dependencies on any earlier released Security Patch Cluster

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

CVE-2014-6271 CVE-2014-7169 CVE-2014-7186 CVE-2014-7187 CVE-2014-6277 CVE-2014-6278

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

DocuSP v5

There are two versions of this patch for DocuSP v5.
Patch 126547-07 is intended for Xerox printer products running the DocuSP software releases on DFE platforms with the x86 CPU.
Patch 126546-07 is intended for products running on DFE platforms with the SPARC CPU.

The patch has been tested with recent versions of the DocuSP v5 Release, but has not been tested with all previously-issued versions of the DocuSP v5 software releases. However, there should not be any problems on these releases.

Tested Releases: X86 release CP.54.A0.63.86; SPARC release CP.54.B3.93

The Xerox Customer Service Engineer (CSE)/Analyst can confirm the patch has successfully installed by typing this command at the root password prompt:

patchadd –p | grep 126546-07 (SPARC)

Or

patchadd –p | grep 126547-07 (x86)

FFPS v6, v7, v8, v9

The Oracle Patch 126547-07 is intended for any Xerox printer products running the FFPS v6, v7, v8 or v9 software releases. The patch has been tested with current versions of these releases but has not been tested with all previously-issued versions of these software releases. However, there should not be any problems on these releases.

Tested Releases: CP.93.E1.14a; CP82.C3.31; CP 73.D2.33; CP 73.C5.11

The Xerox Customer Service Engineer (CSE)/Analyst can confirm the patch has successfully installed by typing this command at the root password prompt:

patchadd –p | grep 126547-07 (x86)

Patch Install

The install of these Security patches must be performed by a Xerox 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. The method available for delivery is an FTP transfer to the DocuSP or FFPS system or writing the patch cluster to DVD/USB media.

Once the Security patch is ready for customer delivery it is made available on the CFO Web site. The Xerox CSE/Analyst can download and prepare for the install by writing the Security patch into a known directory on the FFPS system, or on DVD/USB media. The FFPS Security Patch is delivered as a ZIP archive file. Once the patch has been prepared on media an install script can be run to perform the install.

The Security patch cluster is delivered as a ZIP. To confirm the file size and check sum of these files on Windows and Solaris, please contact FFPS CFO for this information.

Disclaimer