Xerox Security Bulletin XRX14-003

Software Release to Eliminate SQL Injection Vulnerability

v1.0
04/22/14

Background

An SQL injection vulnerability exists that, if exploited, could allow remote attackers to insert arbitrary code into the applicable software application. If successful, an attacker could make unauthorized changes to, damage or delete database tables and values.

A set of software "hotfixes" for the software application listed below have been provided that removes this vulnerability. These "hotfixes" are designed to be installed by the customer. The software "hotfixes" are contained in .tar files for Linux and Solaris or .exe/. jar files for Windows and can be accessed via the link to the DocuShare Support & Software Page (http://www.support.xerox.com/support/xerox-docushare/software/enus.htm) or via the links following this bulletin announcement on www.xerox.com /security:

Once you access the DocuShare Support & Software Page select the applicable operating system from the list below; the page displayed will contain the link to the applicable "hotfix" file:

- Windows Server 2003 & Windows Server 2008:
  DocuShare 6.5.3 Patch 6 -- DocuShare 6.5.3 Patch 6 Hotfix 2 for Windows Server
- Windows Server 2008 x64 & Windows Server 2008 x64:
  DocuShare 6.5.3 Patch 6 -- DocuShare 6.5.3 Patch 6 Hotfix 2 for Windows Server
  DocuShare 6.6.1 Update 1-- DocuShare 6.6.1 Update 1 Hotfix 24 for Windows Server
  DocuShare 6.6.1 Update 2 -- DocuShare 6.6.1 Update 2 Hotfix 3 for Windows Server
- Windows Server 2012 R2 & Windows Server 2012 x64:
  DocuShare 6.6.1 Update 1-- DocuShare 6.6.1 Update 1 Hotfix 24 for Windows Server
  DocuShare 6.6.1 Update 2 -- DocuShare 6.6.1 Update 2 Hotfix 3 for Windows Server
- Linux:
  DocuShare 6.5.3 Patch 6 -- DocuShare 6.5.3 Patch 6 Hotfix 2 for Linux
  DocuShare 6.6.1 Update 2 -- DocuShare 6.6.1 Update 2 Hotfix 3 for Linux
- Unix & Solaris:
  DocuShare 6.5.3 Patch 6 -- DocuShare 6.5.3 Patch 6 Hotfix 2 for Solaris UNIX
  DocuShare 6.6.1 Update 2 -- DocuShare 6.6.1 Update 2 Hotfix 3 for Solaris UNIX

These software "hotfixes" are classified as a **Critical** update.

Please follow the instructions starting on page 3 for each affected DocuShare version to install the appropriate software "hotfix."

Applicability

This bulletin applies to the following software product:

DocuShare 6.5.3 Patch 6 / 6.6.1Update 1 / 6.6.1 Update 2

Acknowledgment

Xerox wishes to thank Secunia Research (http://www.secunia.com) for identifying this vulnerability.

Instructions (What must to be done If I have one of the affected DocuShare versions?)

Determine what actions, if any, need to be performed to prep your server for installation of the appropriate software "hotfix:"

1. Determine the current DocuShare version on your server by clicking on the DocuShare Home page "About DocuShare."
    a. For DocuShare 6.6.1, the "Updates:" line in the About DocuShare page will show if you have Update 1 and/or Update 2 (ds661update 1 and/or ds661update2).
2. From the directions in the Installation Action Table on Page 3 for the affected DocuShare version determine what action, if any, has to be taken before the "hotfix" linked on page 1 can be installed.
3. Perform the indicated action to get your server ready to install the "hotfix."
4. Once your server is ready to install the "hotfix," follow the Software Installation Instructions to install the "hotfix" on your server.

Installation Action Table

The following table indicates what actions, if necessary, are the affected client/server:

	If Your DocuShare Version Is:	Next step:
1	Less than 6.5.3 Patch 6	Upgrade to 6.5.3 Patch 6
2	6.5.3 Patch 6	Install the appropriate "hotfix"[1] – **DocuShare 6.5.3 Patch 6 Hotfix 2**
3	6.6.0	Update to either 6.6.1 Update 1[2] or 6.6.1 Update 2
4	6.6.1 Update 1	Install the appropriate "hotfix" for 6.6.1 Update 1[2] – **DocuShare 6.6.1 Update 1 Hotfix 24**
5	6.6.1 Update 2	Install the appropriate "hotfix" for 6.6.1 Update 2[1] – **DocuShare 6.6.1 Update 2 Hotfix 3**

To install a DocuShare release or one of the "hotfixes" that resolves the vulnerability documented in this bulletin follow the appropriate instructions for your operating system (Unix, Linux, Solaris or Windows Server) in the DocuShare Installation Guide linked to this bulletin below. The releases are available from the DocuShare Support & Software Page (http://www.support.xerox.com/support/xerox-docushare/software/enus.htm) by following the same directions for accessing the "hotfixes" described on page 1.

DocuShare Installation Guide.pdf

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.

The information in this bulletin is subject to change without notice.

[1] There are separate "hotfixes" for servers that have the Unix, Linux, Solaris or Windows Server operating systems. Make sure that you select the proper hotfix for your operating system.
[2] Windows Server operating system only.