DocuShare Security Bulletin XRX22-008

Special Bulletin Regarding CVE-2007-5909 and CVE-2007-5910
Bulletin Date: February 24, 2022
Version 1.0

1.0 Background

The security vulnerability CVE-2007-5909, is a vulnerability which allows remote attackers to execute arbitrary code via a crafted (1) AG file to kpagrdr.dll, (2) AW file to awsr.dll, (3) DLL or (4) EXE file to exesr.dll, (5) DOC file to mwsr.dll, (6) MIF file to mifsr.dll, (7) SAM file to lasr.dll, or (8) RTF file to rtfsr.dll. NOTE: the WPD (wp6sr.dll) vector is covered by CVE-2007-5910.

Details of above CVE's can be found here:

- NIST National Vulnerability Database
  https://nvd.nist.gov/vuln/detail/CVE-2007-5909
  https://nvd.nist.gov/vuln/detail/CVE-2007-5910

Xerox would like to acknowledge Exodus Intelligence in reporting the issue.

2.0 Purpose

DocuShare uses affected DLLs to perform indexing of Word Perfect (.wpd) or AMI Pro (.sam) files. This patch for the vulnerability has disabled Indexing of these files. This will also mean that content in these file types cannot be searched.

3.0 Products

Product	CVE-2007-5909 and CVE-2007-5910 Impact
DocuShare Go	No Impact
DocuShare 6.6.1	Affected – Xerox has developed a hotfix – **Available here**
DocuShare 7.0	Affected – Xerox has developed a hotfix – **Available here**
DocuShare 7.5	Affected – Xerox has developed a hotfix – **Available here**
DocuShare Flex 2.6	No Impact
DocuShare Flex 2.8	No Impact

*I have DocuShare in the Xerox Cloud, what should I do to protect myself?

*If your DocuShare servers are hosted with Xerox, we've got you covered. The update will be applied before close of business today.

For questions, please contact DocuShare Support at docushare.support@xerox.com or call 1-800-835-9013.