



XEROX SECURITY BULLETIN XRX08-002

Information on a Vulnerability in DocuWorks

Here we provide information on a vulnerability in DocuWorks and a security update solution for DocuWorks users.

1. Summary

A vulnerability related to Microsoft Security Bulletin MS07-061** has been identified in the following Xerox software: DocuWorks, DocuWorks Viewer Light and DocuWorks Viewer Light for Web. An attacker could exploit this vulnerability and execute arbitrary code when a specially formatted DocuWorks file is opened and a specific operation is performed. Xerox strongly recommends that users of the affected versions update their product installations.

2. Affected DocuWorks Software and their Versions

English Version

Product Type	Software	Version	
		Version 5.x	Version 6.x
Product for Sales	DocuWorks	5.0.5a and earlier	6.2.2 and earlier
Free Viewer Software	DocuWorks Viewer Light		
	DocuWorks Viewer Light for Web		

French Version

Product Type	Software	Version	
		Version 5.x	Version 6.x
Product for Sales	DocuWorks	/	6.2.2 and earlier
Free Viewer Software	DocuWorks Viewer Light		
	DocuWorks Viewer Light for Web		



3. Solution

English Version

Product Type	Software	Version	
		Version 5.x	Version 6.x
Product for Sales	DocuWorks	Please update to DocuWorks 5.0.6. (Click here for download.)	Please update to DocuWorks 6.2.3. (Click here for download.)
Free Viewer Software	DocuWorks Viewer Light	Please update to DocuWorks Viewer Light 6.2.3 ^{*2} . (Click here for download.)	
	DocuWorks Viewer Light for Web		

French Version

Product Type	Software	Version		
		Version 5.x	Version 6.x	
Product for Sales	DocuWorks	/	Please update to DocuWorks 6.2.3. (Click here for download.)	
Free Viewer Software	DocuWorks Viewer Light		/	Please update to DocuWorks Viewer Light 6.2.3 ^{*2} . (Click here for download.)
	DocuWorks Viewer Light for Web			

It is also recommended that customers who use Microsoft® Windows® XP or Microsoft® Windows Server® 2003 apply the Microsoft update^{*1} described in Microsoft Security Bulletin MS07-061.

4. Other information

Even after customers have installed the update, the vulnerability will still exist in a self-extract DocuWorks file^{*3} created using an affected DocuWorks version. Please do not open a self-extract DocuWorks file with an unknown owner.

*1 For more information on the vulnerability MS07-061 and the security update solution, see the following Microsoft Security Bulletin:

<http://www.microsoft.com/technet/security/bulletin/ms07-061.msp>

<http://www.microsoft.com/france/technet/security/bulletin/ms07-061.msp>

*2 DocuWorks Viewer Light for Web 6.2.3 is included in DocuWorks Viewer Light 6.2.3 installer.

*3 An executable form of a DocuWorks file (extension: exe) that can be displayed or printed on a system in which DocuWorks is not installed. Includes both a DocuWorks file and DocuWorks Viewer Light.

Disclaimer

The information provided in this document 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 document including, without limitation, direct,



indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.



Information sur une vulnérabilité dans DocuWorks

Le xx janvier 2008

Le présent document contient de l'information sur une vulnérabilité dans DocuWorks et sur une mise à jour de sécurité pour les utilisateurs de DocuWorks.

1. Résumé

Une vulnérabilité décrite dans le Bulletin de sécurité MS07-061 de MicrosoftTM a été identifiée dans le logiciel suivant de Xerox : DocuWorks, Visionneuse légère DocuWorks et Visionneuse légère DocuWorks pour le Web. Une personne malveillante pourrait exploiter cette vulnérabilité et exécuter un code arbitraire lorsqu'un fichier DocuWorks spécialement formaté est ouvert et qu'une opération spécifique est exécutée. Xerox recommande fortement que les utilisateurs des versions concernées mettent à jour l'installation de leur produit.

2. Logiciel DocuWorks concerné

Version française

Type de produit	Logiciel	Version	
		Version 5.x	Version 6.x
Produit pour la vente	DocuWorks	/	6.2.2 et versions précédentes
Logiciel gratuit	Visionneuse DocuWorks légère		
Visionneuse	Visionneuse DocuWorks légère pour le Web		

Version anglaise

Type de produit	Logiciel	Version	
		Version 5.x	Version 6.x
Produit pour la vente	DocuWorks	5.0.5a et versions précédentes	6.2.2 et versions précédentes
Logiciel gratuit	DocuWorks Viewer Light		
Visionneuse	DocuWorks Viewer Light for Web		

3. Solution

Version française

Type de produit	Software	Version	
		Version 5.x	Version 6.x
Produit pour la vente	DocuWorks	/	Veillez installer la mise à jour DocuWorks 6.2.3. (Cliquez ici pour télécharger.)
Logiciel gratuit Visionneuse	Visionneuse DocuWorks légère Visionneuse DocuWorks légère pour le Web		Veillez installer la mise à jour Visionneuse légère 6.2.3 ^{*2} . (Cliquez ici pour télécharger.)

Version anglaise

Product Type	Software	Version	
		Version 5.x	Version 6.x
Produit pour la vente	DocuWorks	Veillez installer la mise à jour DocuWorks 5.0.6. (Cliquez ici pour télécharger.)	Veillez installer la mise à jour 6.2.3. (Cliquez ici pour télécharger.)
Logiciel gratuit Visionneuse	DocuWorks Viewer Light DocuWorks Viewer Light for Web	Veillez installer la mise à jour DocuWorks Viewer Light 6.2.3 ^{*2} . (Cliquez ici pour télécharger.)	

Nous recommandons aux clients qui utilisent Microsoft® Windows® XP ou Microsoft® Windows Server® 2003 d'installer la mise à jour ^{*1} décrite dans le Bulletin de sécurité MS07-061 de Microsoft.

4. Autre information

Même après que les clients ont installé la mise à niveau, le problème de vulnérabilité sera toujours présent dans le cas d'un fichier auto-extractible DocuWorks file^{*3} créé à l'aide d'une version « infectée » de DocuWorks.

Veillez ne pas ouvrir de fichier auto-extractible DocuWorks provenant d'un auteur inconnu.

^{*1} Pour plus d'information sur la vulnérabilité MS07-061 et sur la mise à jour de sécurité, consultez le Bulletin de sécurité suivant de Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms07-061.mspx>

<http://www.microsoft.com/france/technet/security/bulletin/ms07-061.mspx>

^{*2} Visionneuse DocuWorks légère pour le Web 6.2.3 est inclus dans l'installation de Visionneuse DocuWorks légère 6.2.3.

^{*3} Forme exécutable d'un fichier DocuWorks (extension : exe) qui peut être affiché ou imprimé sur un système sur lequel DocuWorks n'est pas installé. Inclut un fichier DocuWorks et Visionneuse DocuWorks légère.



Avis de non-responsabilité

L'information contenue dans le présent document est fournie « tel quelle » sans quelque garantie que ce soit. Xerox Corporation décline toute responsabilité concernant toutes les garanties, expresses ou implicites, incluant les garanties de qualité marchande et d'adaptation à un usage particulier. En aucun cas Xerox Corporation ne sera tenue responsable de quelque dommage que ce soit résultant de l'utilisation ou du non-respect par l'utilisateur de l'information contenue dans le présent document incluant, sans s'y limiter, les dommages directs, indirects, corrélatifs ou consécutifs, les pertes de profits ou les dommages spéciaux, même si Xerox Corporation a été informée de la possibilité de tels dommages. Comme certaines juridictions ne permettent pas l'exclusion ou la limitation de la responsabilité pour les dommages indirects, il se peut que cette limitation ne s'applique pas, le cas échéant.