Xerox Product Response to CERT® Vulnerability Note VU#218526: *Microsoft Windows contains vulnerability in Window Management API (MS04-032)*

Audience and Purpose

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to US-CERT® Vulnerability Note VU# 218526, issued by US-CERT® on October 13th, 2004. The following sections provide excerpts from the US-CERT® Technical Cyber Security Alert and the corresponding Xerox response.

Background

The United States-Computer Emergency Readiness Team (US-CERT) is a partnership between the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS) and the private sector. US-CERT provides individuals and organizations with access to valuable educational resources as well as up-to-date computer security information via the National Cyber Alert System.

US-CERT® Vulnerability Note VU# 218526 describes a vulnerability in the Microsoft Windows window application programming interfaces (APIs) that could allow a local attacker to gain elevated privileges on a vulnerable system.

Xerox Product Response

The table below lists various products and their positions with respect to these vulnerabilities. The table will be updated with product information as it becomes available.

Product	Response to US-CERT® Vulnerability Note VU# 218526
CentreWare Network Scanning Services	CentreWare Network Scanning Services is not directly affected by this vulnerability. Operating systems on which CentreWare Network Scanning Services reside may be affected. We recommend that our customers install the latest operating system security patches.
CentreWare Network Services	CentreWare Network Services is not directly affected by this vulnerability. Operating systems on which CentreWare Network Services reside may be affected. We recommend that our customers install the latest operating system security patches.
CopyCentre C20	The CopyCentre C20 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.

© 2004, 2005 Xerox Corporation. All rights reserved.

Product	Response to US-CERT® Vulnerability Note VU# 218526
DigiPath	DigiPath is affected by this vulnerability. DigiPath 3.0/4.x customers should use the following instructions to update your DigiPath system: **Instructions for using Windows Update on DigiPath version 3.0/4.x** 1. Ensure that a TapeWare system backup exists. 2. Create a new Microsoft System Restore point (**not** available in Windows Server 2003). – Select "**Start"** and go to "**Programs>Accessories>System Tools>System Restore"**. – Follow the instructions to create a new restore point. 3. On a weekly basis, run Windows Update: **Note:** Operating System and Internet Explorer Service Packs are **not** to be installed via this process. When selecting "Review and Install Updates", remove the service pack from the list of downloads. Continue with the rest of the patches by selecting "**Install Now**". a. Open up Windows Internet Explorer. b. From the Tools menu, select "**Windows Update**". c. If prompted to install the latest Windows Update software, select **[Yes].** Then select **[Yes]** to reboot your machine. Then access Windows Update again per steps 3a and 3b. d1. If running Windows Update version 4 (version listed in URL address, for example http://v4.windowsupdate.microsoft.com), perform the following steps: 1. Select "**Scan for Updates**" in the main center window. 2. In the left window pane, select "**Critical Updates and Service Packs**". 3. Select "**Review and Install Updates**". 4. Select **[Install Now]** to download all the Microsoft critical updates needed for your system. 5. Select **[Accept]** to accept the Microsoft license agreement. 6. The patches will be downloaded and installed. 7. If prompted, select **[Yes]** to restart your system. d2. If running Windows Update version 5 (http://v5.windowsupdate.microsoft.com), perform the following steps: 1. Select Custom Install. 2. Do NOT download and install Windows XP SP2. 3. Select "Review other Updates". 4. Select "Go to Install updates". 5. Select "Install". 6. The patches will be downloaded and installed. 7. Select **[Yes]** to accept the Microsoft license agreement. 8. Select **[No]** if you get the Microsoft GDI+ Detection Tool message. 9. Select **[Restart Now]** to restart your system.
DocuColor 2240/1632	The DocuColor 2240/1632 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.
DocuColor 3535 with EFI Network Controller	DocuColor 3535 with EFI Network Controller is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.

© 2004, 2005 Xerox Corporation. All rights reserved.

Product	Response to US-CERT® Vulnerability Note VU# 218526
DocuColor Windows 2000 based products with Creo front-ends: • **DocuColor 3535 with CXP3535** • **DocuColor 6060/5252/2060/2045 with CXP6000** • **DocuColor 5252/2045 with CXP5000**	DocuColor Windows 2000 based products with Creo front-ends are affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative. **Patch installation instructions:** 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
DocuColor Windows NT based products with Creo front-ends: • **DocuColor 2060/2045 with CSX2000**	DocuColor Windows NT based products with Creo front-ends are affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative. **Patch installation instructions:** 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
DocuColor Windows XP Professional SP1 based products with Creo front-ends: • **DocuColor 3535 with CXP3535e**	DocuColor Windows XP Professional SP1 based products with Creo front-ends are affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative. **Patch installation instructions:** 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
DocuColor Windows XP Professional SP2 based products with Creo front-ends: ▪ **DocuColor 3535 with CXP3535e**	DocuColor Windows XP Professional SP2 based products with Creo front-ends include the fix and are not, therefore, affected by this vulnerability.
DocuColor with EFI Splash front-ends: • **DocuColor 12 with G640** • **DocuColor 3535 with G3535**	DocuColor products with EFI Splash front-ends are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.

© 2004, 2005 Xerox Corporation. All rights reserved.

Product	Response to US-CERT® Vulnerability Note VU# 218526
Document Centre Xerox WIA Driver for Microsoft® Windows XP®	Document Centre Xerox WIA Driver for Microsoft Windows XP is not directly affected by this vulnerability. Operating systems on which Document Centre Xerox WIA Driver for Microsoft Windows XP resides may be affected. We recommend that our customers install the latest operating system security patches.
DocuPrint N Series products	DocuPrint N Series products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products are Sun-based and are not, therefore, affected by this vulnerability.
DocuSP-based products	DocuSP-based products are Sun Solaris-based and are not, therefore, affected by this vulnerability.
FaxCentre F12	The FaxCentre F12 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.
FlowPort	FlowPort is not directly affected by this vulnerability. Operating systems on which Flowport resides may be affected. We recommend that our customers install the latest operating system security patches.

© 2004, 2005 Xerox Corporation. All rights reserved.

Product	Response to US-CERT® Vulnerability Note VU# 218526
FreeFlow Prepress Suite	FreeFlow 2.0 Prepress Suite is affected by this vulnerability. FreeFlow 2.0 Prepress Suite customers should use the following instructions to update your FreeFlow system: **Instructions for using Windows Update on FreeFlow version 2.0** 1. Ensure that a TapeWare system backup exists. 2. Create a new Microsoft System Restore point (**not** available in Windows Server 2003). – Select "**Start"** and go to "**Programs>Accessories>System Tools>System Restore"**. – Follow the instructions to create a new restore point. 3. On a weekly basis, run Windows Update: **Note:** Operating System and Internet Explorer Service Packs are **not** to be installed via this process. When selecting "Review and Install Updates", remove the service pack from the list of downloads. Continue with the rest of the patches by selecting "**Install Now**". a. Open up Windows Internet Explorer. b. From the Tools menu, select "**Windows Update**". c. If prompted to install the latest Windows Update software, select **[Yes].** Then select **[Yes]** to reboot your machine. Then access Windows Update again per steps 3a and 3b. d1. If running Windows Update version 4 (version listed in URL address, for example http://v4.windowsupdate.microsoft.com), perform the following steps: 1. Select "**Scan for Updates**" in the main center window. 2. In the left window pane, select "**Critical Updates and Service Packs**". 3. Select "**Review and Install Updates**". 4. Select **[Install Now]** to download all the Microsoft critical updates needed for your system. 5. Select **[Accept]** to accept the Microsoft license agreement. 6. The patches will be downloaded and installed. 7. If prompted, select **[Yes]** to restart your system. d2. If running Windows Update version 5 (http://v5.windowsupdate.microsoft.com), perform the following steps: 1. Select Custom Install. 2. Do NOT download and install Windows XP SP2. 3. Select "Review other Updates". 4. Select "Go to Install updates". 5. Select "Install". 6. The patches will be downloaded and installed. 7. Select **[Yes]** to accept the Microsoft license agreement. 8. Select **[No]** if you get the Microsoft GDI+ Detection Tool message. 9. Select **[Restart Now]** to restart your system.
FreeFlow SMARTsend	FreeFlow SMARTsend is not directly affected by this vulnerability. Operating systems on which SMARTsend resides may be affected. We recommend that our customers install the latest operating system security patches.
Phaser products	Phaser products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.

© 2004, 2005 Xerox Corporation. All rights reserved.

Product	Response to US-CERT® Vulnerability Note VU# 218526
WorkCentre M15 **WorkCentre M20/M20i** **WorkCentre M24** **WorkCentre M35** **WorkCentre M45** **WorkCentre M55** **WorkCentre PE16** **WorkCentre Pro 35** **WorkCentre Pro 45** **WorkCentre Pro 55** **WorkCentre Pro 65** **WorkCentre Pro 75** **WorkCentre Pro 90** **WorkCentre Pro 423** **WorkCentre Pro 428** **WorkCentre Pro 32 Color** **WorkCentre Pro 40 Color** **WorkCentre Pro C2128** **WorkCentre Pro C2636** **WorkCentre Pro C3545**	These WorkCentre products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.
Xerox 1010/2101 Windows NT Copy Server	The Xerox 1010/2101 Windows NT Copy Server is not affected by this vulnerability.
Xerox products with EFI Windows NT based front ends with Fiery Advanced Controller Interface (FACI): • **DocuColor 12 with X12** • **DocuColor 12 with EX12** • **DocuColor 12 with XP12** • **DocuColor 40 with X40** • **DocuColor 2045/2060 with EX2000** • **DocuColor 2045/2060/5252 with EX2000d** • **DocuColor 2045/2060 with EX2000v** • **Xerox 1010 with EX1010**	Xerox products with EFI Windows NT based front ends with FACI are affected by this vulnerability. A patch can be downloaded by visiting the Microsoft Security Bulletin site at http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx.

© 2004, 2005 Xerox Corporation. All rights reserved.

Product	Response to US-CERT® Vulnerability Note VU# 218526
Xerox products with EFI Windows NT based front ends without Fiery Advanced Controller Interface (FACI): • **DocuColor 12 with X12** • **DocuColor 12 with EX12** • **DocuColor 12 with XP12** • **DocuColor 40 with X40** • **Xerox 1010 with EX1010**	Xerox products with EFI Windows NT based front ends without FACI are affected by this vulnerability. A patch can be downloaded by visiting the Microsoft Security Bulletin site at http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx.

Contact
For additional information or clarification on any of the product information given here, contact Xerox support.

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 no allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

© 2004, 2005 Xerox Corporation. All rights reserved.