

## Xerox Product Response to US-CERT® Technical Cyber Security Alert TA05-362A: Microsoft Windows Metafile Handling Buffer Overflow

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [US-CERT® Technical Cyber Security Alert TA05-362A](#), issued by US-CERT® on December 28<sup>th</sup>, 2005. 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 (NCSA) 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® Technical Cyber Security Alert TA05-362A](#) states that Microsoft Windows is vulnerable to remote code execution via an error in handling files using the Windows Metafile image format. A remote, unauthenticated attacker may be able to execute arbitrary code if the user is persuaded to view a specially crafted Windows Metafile.

### 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 <a href="#">US-CERT® Technical Cyber Security Alert TA05-362A</a>
<b>CentreWare Network Scanning Services</b>	CentreWare Network Scanning Services is not directly affected by these vulnerabilities. Operating systems on which CentreWare Network Scanning Services reside may be affected. We recommend that our customers install the latest operating system security patches.
<b>CentreWare Network Services</b>	CentreWare Network Services is not directly affected by these vulnerabilities. Operating systems on which CentreWare Network Services reside may be affected. We recommend that our customers install the latest operating system security patches.
<b>CopyCentre 123 CopyCentre 128 CopyCentre 133 CopyCentre M20</b>	These CopyCentre products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.
<b>DocuColor 2240/1632</b>	The DocuColor 2240/1632 is not Microsoft Windows-based and is not, therefore, affected by these vulnerabilities.
<b>DocuColor 3535 with EFI Network Controller</b>	DocuColor 3535 with EFI Network Controller is not Microsoft Windows-based and is not, therefore, affected by these vulnerabilities.
<b>DocuColor with EFI Splash front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 12 with G640</li> <li>• DocuColor 3535 with G3535</li> </ul>	DocuColor products with EFI Splash front-ends are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.
<b>Document Centre products (200, 300, 400 and 500 Series)</b>	Document Centre products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.

<b>Product</b>	<b>Response to <a href="#">US-CERT® Technical Cyber Security Alert TA05-362A</a></b>
<b>Document Centre Xerox WIA Driver for Microsoft® Windows XP®</b>	Document Centre Xerox WIA Driver for Microsoft Windows XP is not directly affected by these vulnerabilities. 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.
<b>DocuPrint N Series products</b>	DocuPrint N Series products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.
<b>DocuPrint NPS/IPS Series products</b>	DocuPrint NPS/IPS Series products are Sun-based and are not, therefore, affected by these vulnerabilities.
<b>DocuSP-based products</b>	DocuSP-based products are Sun Solaris-based and are not, therefore, affected by these vulnerabilities.
<b>FaxCentre F12</b>	The FaxCentre F12 is not Microsoft Windows-based and is not, therefore, affected by these vulnerabilities.
<b>FlowPort</b>	FlowPort is not directly affected by these vulnerabilities. Operating systems on which Flowport resides may be affected. We recommend that our customers install the latest operating system security patches.

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA05-362A</a>
<p><b>FreeFlow™ Makeready, Process Manager, and Web Services (includes DigiPath)</b></p>	<p>FreeFlow Makeready, Process Manager, and Web Services (including DigiPath) are affected by this vulnerability. We recommend that our customers install the latest "High Priority" operating system security patches using the following instructions:</p> <p><b><u>Instructions for using Windows Update on FreeFlow Makeready, Process Manager, and Web Services (includes DigiPath)</u></b></p> <ol style="list-style-type: none"> <li>1. Ensure that a TapeWare system backup exists.</li> <li>2. Create a new Microsoft System Restore point (<b>not</b> available in Windows Server 2003).               <ul style="list-style-type: none"> <li>- Select "<b>Start</b>" and go to "<b>Programs&gt;Accessories&gt;System Tools&gt;System Restore</b>".</li> <li>- Follow the instructions to create a new restore point.</li> </ul> </li> <li>3. On a weekly basis, run Windows Update:               <p>The Windows Update web site and software are maintained and updated at the discretion of Microsoft. The update process can also be affected by the operating system, version of Windows Update software currently installed on the system, and even the manner in which Windows Update is launched. As such, the Windows Update process cannot be documented in a directive manner. Instead, the following guidelines should be followed when running Windows Update:</p> <ul style="list-style-type: none"> <li>• If the Windows Update web site prompts to install a newer version of the Windows Update software, follow the on-screen installation instructions to install the new version of software.                   <p><b>NOTE: If you install a newer version of Windows Update software, you will have to run Windows update again to install the updates.</b></p> </li> <li>• When running Windows Update, always select the <b>Custom Install</b> option. This option will allow for the de-selection of unsupported components, such as Service Packs.                   <p><i>NOTE: For a current listing of the supported Service Packs and updates, please refer to the most recent <a href="#">FreeFlow™/DigiPath Microsoft Patch Summary</a>.</i></p> <p><b>NOTE: When selecting updates from "Custom Installs" ensure all unsupported service packs are removed from the list of downloads before installing the updates.</b></p> </li> <li>• Operating System and Internet Explorer Service Packs are <b>not</b> to be installed via this process unless otherwise indicated.</li> </ul> </li> <li>4. Run Windows Update. The application can be launched from either of the following interfaces:               <ul style="list-style-type: none"> <li>• The Windows Start menu (select [Windows Update])</li> <li>• Internet Explorer (select [Tools: Windows Update])</li> </ul> </li> </ol>
<p><b>FreeFlow Output Manager FreeFlow Print Manager FreeFlow SMARTsend™</b></p>	<p>These FreeFlow products are not directly affected by these vulnerabilities. Operating systems on which they reside may be affected. We recommend that our customers install the latest operating system security patches.</p>
<p><b>Phaser products</b></p>	<p>Phaser products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA05-362A</a>
<p> <b>WorkCentre 123</b>  <b>WorkCentre 128</b>  <b>WorkCentre 133</b>  <b>WorkCentre C2424</b>  <b>WorkCentre M15</b>  <b>WorkCentre M20/M20i</b>  <b>WorkCentre M24</b>  <b>WorkCentre M35</b>  <b>WorkCentre M45</b>  <b>WorkCentre M55</b>    <b>WorkCentre PE16</b>    <b>WorkCentre Pro 35</b>  <b>WorkCentre Pro 45</b>  <b>WorkCentre Pro 55</b>  <b>WorkCentre Pro 65</b>  <b>WorkCentre Pro 75</b>  <b>WorkCentre Pro 90</b>  <b>WorkCentre Pro 123</b>  <b>WorkCentre Pro 128</b>  <b>WorkCentre Pro 133</b>  <b>WorkCentre Pro 232</b>  <b>WorkCentre Pro 238</b>  <b>WorkCentre Pro 245</b>  <b>WorkCentre Pro 255</b>  <b>WorkCentre Pro 265</b>  <b>WorkCentre Pro 275</b>  <b>WorkCentre Pro 423</b>  <b>WorkCentre Pro 428</b>  <b>WorkCentre Pro 32 Color</b>  <b>WorkCentre Pro 40 Color</b>    <b>WorkCentre Pro C2128</b>  <b>WorkCentre Pro C2636</b>  <b>WorkCentre Pro C3545</b> </p>	<p>These WorkCentre products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.</p>
<p><b>Xerox 1010/2101 Windows NT Copy Server</b></p>	<p>The Xerox 1010/2101 Windows NT Copy Server is not affected by this vulnerability.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA05-362A</a>
<p><b>Xerox products with EFI Windows NT based front ends with Fiery Advanced Controller Interface (FACI):</b></p> <ul style="list-style-type: none"> <li>• DocuColor 12 with X12</li> <li>• DocuColor 12 with EX12</li> <li>• DocuColor 12 with XP12</li> <li>• DocuColor 40 with X40</li> <li>• DocuColor 2045/2060 with EX2000</li> <li>• DocuColor 2045/2060/5252 with EX2000d</li> <li>• DocuColor 2045/2060 with EX2000v</li> <li>• Xerox 1010 with EX1010</li> </ul>	<p>Xerox products with EFI Windows NT based front ends with FACI are not affected by this vulnerability.</p>
<p><b>Xerox products with EFI Windows NT based front ends <u>without</u> Fiery Advanced Controller Interface (FACI):</b></p> <ul style="list-style-type: none"> <li>• DocuColor 12 with X12</li> <li>• DocuColor 12 with EX12</li> <li>• DocuColor 12 with XP12</li> <li>• DocuColor 40 with X40</li> <li>• Xerox 1010 with EX1010</li> </ul>	<p>Xerox products with EFI Windows NT based front ends <u>without</u> FACI are not affected by this vulnerability.</p>
<p><b>Xerox products with EFI Windows XPe based front ends with Fiery Advanced Controller Interface (FACI):</b></p> <ul style="list-style-type: none"> <li>• DocuColor 12 with X12/EX12/XP12 (customer purchased s/w option)</li> <li>• DocuColor 3535 with EX3535*</li> <li>• DocuColor 5252 with EXP5000</li> <li>• DocuColor 6060 with EXP6000</li> <li>• DocuColor 8000 with EXP8000</li> <li>• Phaser EX7750</li> <li>• Xerox 2101 with EX2101</li> </ul>	<p>Xerox products with EFI Windows XPe based front-ends with FACI are affected by this vulnerability. Follow the System Update instructions below, which will direct you to a website from which all patches can be downloaded and installed automatically:</p> <p>Select Start --&gt; All Program --&gt; System Update</p> <p style="text-align: center;">-----</p> <p>* <b>DocuColor 3535 with EX3535 v1.0:</b> System Update is available after the appropriate patch has been installed. The Systems Updates Patch can be found at <a href="http://www.support.xerox.com/go/getfile.asp?Xlang=en_US&amp;XCntry=USA&amp;objid=44488&amp;EULA=0&amp;prodId=DC_3535&amp;Family=DocuColor&amp;ripld=XRIP_Fiery_EX3535&amp;langs=English%20(US)&amp;plats=Windows%20XP&amp;Xtype=download">http://www.support.xerox.com/go/getfile.asp?Xlang=en_US&amp;XCntry=USA&amp;objid=44488&amp;EULA=0&amp;prodId=DC_3535&amp;Family=DocuColor&amp;ripld=XRIP_Fiery_EX3535&amp;langs=English%20(US)&amp;plats=Windows%20XP&amp;Xtype=download</a>.</p> <p>When the System Updates Patch has been successfully installed, follow the detailed instructions above.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA05-362A</a>
<b>Xerox products with EFI Windows XPe based front ends <u>without</u> Fiery Advanced Controller Interface (FACI):</b> <ul style="list-style-type: none"><li>• DocuColor 12 with X12/EX12/XP12 (customer purchased s/w option)</li><li>• DocuColor 3535 with EX3535</li><li>• Phaser EX7750</li><li>• Xerox 2101 with EX2101</li></ul>	Xerox products with EFI Windows XPe based front-ends without FACI are affected by this vulnerability. Select 'Check for product update' in the Fiery WebTools utility to install the appropriate patches.

**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 not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.