

## Xerox Product Response to CERT® Vulnerability Note VU#218621: *Microsoft Word buffer overflow in font processing routine (MS05-035)*

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# 218621](#), issued by US-CERT® on July 12<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® Vulnerability Note VU# 218621](#) states that a buffer overflow in the font processing routine used by Microsoft Word may allow a remote attacker to execute code on a vulnerable system.

### Xerox Product Response

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

Product	Response to <a href="#">US-CERT® Vulnerability Note VU# 218621</a>
<b>CentreWare Network Scanning Services</b>	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.
<b>CentreWare Network Services</b>	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.
<b>CopyCentre C20 CopyCentre C123 CopyCentre C128</b>	These CopyCentre products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.
<b>DocuColor 2240/1632</b>	The DocuColor 2240/1632 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.
<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 this vulnerability.
<b>DocuColor Windows 2000 based products with Creo front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 3535 with CXP3535</li> <li>• DocuColor 6060/5252/2060/2045 with CXP6000</li> <li>• DocuColor 5252/2045 with CXP5000</li> </ul>	DocuColor Windows 2000 based products with Creo front-ends are not affected by this vulnerability.

Product	Response to <a href="#">US-CERT® Vulnerability Note VU# 218621</a>
<p><b>DocuColor Windows NT based products with Creo front-ends:</b></p> <ul style="list-style-type: none"> <li>• DocuColor 2060/2045 with CSX2000</li> </ul>	<p>DocuColor Windows NT based products with Creo front-ends are not affected by this vulnerability.</p>
<p><b>DocuColor Windows XP Professional SP1 based products with Creo front-ends:</b></p> <ul style="list-style-type: none"> <li>• DocuColor 3535 with CXP3535e</li> </ul>	<p>DocuColor Windows XP Professional SP1 based products with Creo front-ends are not affected by this vulnerability.</p>
<p><b>DocuColor Windows XP Professional SP2 based products with Creo front-ends:</b></p> <ul style="list-style-type: none"> <li>• DocuColor 3535 with CXP3535e</li> </ul>	<p>DocuColor Windows XP Professional SP2 based products with Creo front-ends are not affected by this vulnerability.</p>
<p><b>DocuColor with EFI Splash front-ends:</b></p> <ul style="list-style-type: none"> <li>• DocuColor 12 with G640</li> <li>• DocuColor 3535 with G3535</li> </ul>	<p>DocuColor products with EFI Splash front-ends are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.</p>
<p><b>Document Centre products (200, 300, 400 and 500 Series)</b></p>	<p>Document Centre products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.</p>
<p><b>Document Centre Xerox WIA Driver for Microsoft® Windows XP®</b></p>	<p>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.</p>
<p><b>DocuPrint N Series products</b></p>	<p>DocuPrint N Series products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.</p>
<p><b>DocuPrint NPS/IPS Series products</b></p>	<p>DocuPrint NPS/IPS Series products are Sun-based and are not, therefore, affected by this vulnerability.</p>
<p><b>DocuSP-based products</b></p>	<p>DocuSP-based products are Sun Solaris-based and are not, therefore, affected by this vulnerability.</p>
<p><b>FaxCentre F12</b></p>	<p>The FaxCentre F12 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.</p>
<p><b>FlowPort</b></p>	<p>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.</p>

Product	Response to <a href="#">US-CERT® Vulnerability Note VU# 218621</a>
<b>FreeFlow Makeready, Process Manager, and Web Services (includes DigiPath)</b>	FreeFlow Makeready, Process Manager, and Web Services (including DigiPath) are not affected by this vulnerability.
<b>FreeFlow SMARTsend™</b>	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.
<b>iGen3 Windows 2000-based Creo Spire Color Server</b>	The iGen3 Windows 2000 based Creo Spire Color Server is not affected by this vulnerability.
<b>Phaser products</b>	Phaser products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.
<b>WorkCentre 232</b> <b>WorkCentre 238</b> <b>WorkCentre 245</b> <b>WorkCentre 255</b> <b>WorkCentre 265</b> <b>WorkCentre 275</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 M123</b> <b>WorkCentre M128</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 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>	These WorkCentre products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.

Product	Response to <a href="#">US-CERT® Vulnerability Note VU# 218621</a>
<b>Xerox 1010/2101 Windows NT Copy Server</b>	The Xerox 1010/2101 Windows NT Copy Server does not use Microsoft Word and is not, therefore, affected by this vulnerability.
<b>Xerox products with EFI Windows NT based front ends with Fiery Advanced Controller Interface (FACI):</b> <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>	Xerox products with EFI Windows NT based front ends with FACI are not affected by this vulnerability.
<b>Xerox products with EFI Windows NT based front ends <u>without</u> Fiery Advanced Controller Interface (FACI):</b> <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>	Xerox products with EFI Windows NT based front ends without FACI are not affected by this vulnerability.
<b>Xerox products with EFI Windows XPe based front ends with 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>• 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>	Xerox products with EFI Windows XPe based front ends with FACI are not affected by this vulnerability.

Product	Response to <a href="#">US-CERT® Vulnerability Note VU# 218621</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 not affected by this vulnerability.

#### 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.