

## **Xerox Product Response to US-CERT® Technical Cyber Security Alert TA04-315A: Buffer Overflow in Microsoft Internet Explorer (MS04-040)**

### **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® Technical Cyber Security Alert TA04-315A](#), issued by US-CERT® on November 10<sup>th</sup>, 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® Technical Cyber Security Alert TA04-315A](#) states that Microsoft Internet Explorer (IE) contains a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code with the privileges of the user running IE.

### **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.

<b>Product</b>	<b>Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a></b>
<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 resides 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 resides may be affected. We recommend that our customers install the latest operating system security patches.
<b>CopyCentre C20</b>	The CopyCentre C20 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a>
<p><b>DigiPath</b></p>	<p>DigiPath is affected by this vulnerability.</p> <p>DigiPath 3.0/4.x customers should use the following instructions to update their DigiPath system:</p> <p><b><u>Instructions for using Windows Update on DigiPath version 3.0/4.x</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><b>Note:</b> Operating System and Internet Explorer Service Packs are <b>not</b> 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 <b>"Install Now"</b>.</p> <ol style="list-style-type: none"> <li>a. Open up Windows Internet Explorer.</li> <li>b. From the Tools menu, select <b>"Windows Update"</b>.</li> <li>c. If prompted to install the latest Windows Update software, select <b>[Yes]</b>. Then select <b>[Yes]</b> to reboot your machine. Then access Windows Update again per steps 3a and 3b.</li> </ol> </li> <li>d1. If running <b>Windows Update version 4</b> (version listed in URL address, for example <a href="http://v4.windowsupdate.microsoft.com">http://v4.windowsupdate.microsoft.com</a>), perform the following steps:             <ol style="list-style-type: none"> <li>1. Select <b>"Scan for Updates"</b> in the main center window.</li> <li>2. In the left window pane, select <b>"Critical Updates and Service Packs"</b>.</li> <li>3. Select <b>"Review and Install Updates"</b>.</li> <li>4. Select <b>[Install Now]</b> to download all the Microsoft critical updates needed for your system.</li> <li>5. Select <b>[Accept]</b> to accept the Microsoft license agreement.</li> <li>6. The patches will be downloaded and installed.</li> <li>7. If prompted, select <b>[Yes]</b> to restart your system.</li> </ol> </li> <li>d2. If running <b>Windows Update version 5</b> (<a href="http://v5.windowsupdate.microsoft.com">http://v5.windowsupdate.microsoft.com</a>), perform the following steps:             <ol style="list-style-type: none"> <li>1. Select Custom Install.</li> <li>2. Do NOT download and install Windows XP SP2.</li> <li>3. Select "Review other Updates".</li> <li>4. Select "Go to Install updates".</li> <li>5. Select "Install".</li> <li>6. The patches will be downloaded and installed.</li> <li>7. Select <b>[Yes]</b> to accept the Microsoft license agreement.</li> <li>8. Select <b>[No]</b> if you get the Microsoft GDI+ Detection Tool message.</li> </ol> </li> <li>9. Select <b>[Restart Now]</b> to restart your system.</li> </ol>
<p><b>DocuColor 1632/2240</b></p>	<p>The DocuColor 1632/2240 products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.</p>
<p><b>DocuColor 3535 with EFI Network Controller</b></p>	<p>DocuColor 3535 with EFI Network Controller is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a>
<p><b>DocuColor Windows 2000 based products with Creo front-ends:</b></p> <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>	<p>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.</p> <p><b><u>Patch installation instructions:</u></b></p> <ol style="list-style-type: none"> <li>1. Exit the Spire application.</li> <li>2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at <a href="http://www.microsoft.com/technet/security/bulletin/ms04-040.msp">http://www.microsoft.com/technet/security/bulletin/ms04-040.msp</a></li> <li>3. Install the appropriate Hot Fix.</li> <li>4. If installation ended with a Restart/reboot prompt, press OK.</li> <li>5. This completes the installation of the Hot Fix.</li> </ol>
<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 affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative.</p> <p><b><u>Patch installation instructions:</u></b></p> <ol style="list-style-type: none"> <li>1. Exit the Spire application.</li> <li>2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at <a href="http://www.microsoft.com/technet/security/bulletin/ms04-040.msp">http://www.microsoft.com/technet/security/bulletin/ms04-040.msp</a></li> <li>3. Install the appropriate Hot Fix.</li> <li>4. If installation ended with a Restart/reboot prompt, press OK.</li> <li>5. This completes the installation of the Hot Fix.</li> </ol>
<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 include the fix and are not, therefore, 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>

<b>Product</b>	<b>Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a></b>
<b>DocuPrint N Series products</b>	DocuPrint N Series products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.
<b>DocuPrint NPS/IPS Series products</b>	DocuPrint NPS/IPS Series products are Sun-based and are not, therefore, affected by this vulnerability.
<b>DocuSP-based products</b>	DocuSP-based products are Sun Solaris-based and are not, therefore, affected by this vulnerability.
<b>FaxCentre F12</b>	The FaxCentre F12 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.
<b>FlowPort</b>	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.

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a>
<p><b>FreeFlow Prepress Suite</b></p>	<p>FreeFlow Prepress Suite 2.0 is affected by this vulnerability.</p> <p>FreeFlow Prepress Suite 2.0 customers should use the following instructions to update their system:</p> <p><b><u>Instructions for using Windows Update on FreeFlow version 2.0</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><b>Note:</b> Operating System and Internet Explorer Service Packs are <b>not</b> 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 <b>"Install Now"</b>.</p> <ol style="list-style-type: none"> <li>a. Open up Windows Internet Explorer.</li> <li>b. From the Tools menu, select <b>"Windows Update"</b>.</li> <li>c. If prompted to install the latest Windows Update software, select <b>[Yes]</b>. Then select <b>[Yes]</b> to reboot your machine. Then access Windows Update again per steps 3a and 3b.</li> </ol> </li> <li>d1. If running <b>Windows Update version 4</b> (version listed in URL address, for example <a href="http://v4.windowsupdate.microsoft.com">http://v4.windowsupdate.microsoft.com</a>), perform the following steps:             <ol style="list-style-type: none"> <li>1. Select <b>"Scan for Updates"</b> in the main center window.</li> <li>2. In the left window pane, select <b>"Critical Updates and Service Packs"</b>.</li> <li>3. Select <b>"Review and Install Updates"</b>.</li> <li>4. Select <b>[Install Now]</b> to download all the Microsoft critical updates needed for your system.</li> <li>5. Select <b>[Accept]</b> to accept the Microsoft license agreement.</li> <li>6. The patches will be downloaded and installed.</li> <li>7. If prompted, select <b>[Yes]</b> to restart your system.</li> </ol> </li> <li>d2. If running <b>Windows Update version 5</b> (<a href="http://v5.windowsupdate.microsoft.com">http://v5.windowsupdate.microsoft.com</a>), perform the following steps:             <ol style="list-style-type: none"> <li>1. Select Custom Install.</li> <li>2. Do NOT download and install Windows XP SP2.</li> <li>3. Select "Review other Updates".</li> <li>4. Select "Go to Install updates".</li> <li>5. Select "Install".</li> <li>6. The patches will be downloaded and installed.</li> <li>7. Select <b>[Yes]</b> to accept the Microsoft license agreement.</li> <li>8. Select <b>[No]</b> if you get the Microsoft GDI+ Detection Tool message.</li> </ol> </li> <li>9. Select <b>[Restart Now]</b> to restart your system.</li> </ol>
<p><b>Phaser products</b></p>	<p>Phaser products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a>
<p> <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 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 this vulnerability.</p>
<p><b>Xerox 1010/2101</b></p>	<p>The Xerox 1010/2101 does not use Internet Explorer and is not, therefore, 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> <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>	<p>Xerox products with EFI Windows NT based front ends without FACI are not affected by this vulnerability because the exploitation occurs when you browse a malicious web site or open an HTML attachment from the e-mail client that guide you to an attacker's web site.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 315A</a>
<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>
<p><b>Xerox products with EFI Windows XPe based front ends <u>without</u> 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>• Phaser EX7750</li> <li>• Xerox 2101 with EX2101</li> </ul>	<p>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.</p>

**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.