

## **Xerox Product Response to CERT<sup>®</sup> Advisory CA-2003-23: RPCSS Vulnerabilities in Microsoft Windows (MS03-039)**

### **Audience and Purpose**

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [CERT<sup>®</sup> Advisory CA-2003-23](#), issued by CERT<sup>®</sup> on September 10<sup>th</sup>, 2003. The following sections provide excerpts from the CERT<sup>®</sup> advisory and the corresponding Xerox response.

### **Background**

The CERT<sup>®</sup> Coordination Center (CERT/CC) is a center of Internet security expertise at the [Software Engineering Institute](#), a federally funded research and development center operated by [Carnegie Mellon University](#). CERT<sup>®</sup> studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

[CERT<sup>®</sup> Advisory CA-2003-23](#) describes three vulnerabilities that affect numerous versions of Microsoft Windows. Two of these vulnerabilities are remotely exploitable buffer overflows that may allow an attacker to execute arbitrary code with system privileges. The third vulnerability may allow a remote attacker to cause a denial of service.

### **Xerox Product Response**

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

Product	Response to <a href="#">CERT Advisory CA-2003-23</a>
DigiPath	<p>DigiPath products are affected by this vulnerability.</p> <p><b><u>Instructions for using Windows Update on DigiPath version 3.0/4.0</u></b></p> <ol style="list-style-type: none"> <li>1. Ensure that a TapeWare system backup exists.</li> <li>2. On a weekly basis, run Windows Update:             <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. If you did not receive this prompt, proceed to step f.</li> <li>d. Open up Windows Internet Explorer.</li> <li>e. From the tools menu, select “<b>Windows Update</b>”.</li> <li>f. Select “<b>Scan for Updates</b>” in the main center window.</li> <li>g. In the left window pane, select “<b>Critical Updates and Service Packs</b>”.</li> <li>h. Select “<b>Review and Install Updates</b>”.</li> <li>i. Select <b>[Install Now]</b> to download all the Microsoft critical updates needed for your system.</li> <li>j. Select <b>[Accept]</b> to accept the Microsoft license agreement.</li> <li>k. The patches will be downloaded and installed.</li> <li>l. If prompted, select <b>[Yes]</b> to restart your system.</li> </ol> </li> </ol> <p><b>Note:</b> Service Packs are <b>not</b> to be installed via this process. When prompted by the Service Pack install message, select “<b>Cancel</b>” to return to the “<b>Install Now</b>” screen, and remove the service pack from the list of downloads. Continue with the rest of the patches by selecting “<b>Install Now</b>”.</p> <p><b><u>Instructions for using Windows Update on DigiPath version 2.1 (Windows NT)</u></b></p> <p><b>Note:</b> DigiPath 1.2 customers can follow these DigiPath 2.1 instructions at their own risk.</p> <ol style="list-style-type: none"> <li>1. Ensure that a TapeWare system backup exists.</li> <li>2. On a weekly basis, run Windows Update:             <ol style="list-style-type: none"> <li>a. Go to URL: <a href="http://windowsupdate.microsoft.com">http://windowsupdate.microsoft.com</a></li> <li>b. The product catalog will be updated for your system.</li> <li>c. Windows Update will customize the product update catalog for your system.</li> <li>d. Only critical update will be automatically selected.</li> <li>e. Select the Download button in the top right window pane.</li> <li>f. Select <b>[Start Download]</b></li> <li>g. Select <b>[Yes]</b> to accept the license agreement.</li> <li>h. The patches will be downloaded and installed.</li> <li>i. If prompted, select <b>[Yes]</b> to restart your system.</li> </ol> </li> </ol>

Product	Response to <a href="#">CERT Advisory CA-2003-23</a>
<b>DocuColor 2060/2045 with CSX2000</b>	<p>DocuColor 2060/2045 with CSX2000 is 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/downloads/details.aspx?FamilyID=71b6135c-f957-4702-b376-2dacce773dc0&amp;DisplayLang=en">http://www.microsoft.com/downloads/details.aspx?FamilyID=71b6135c-f957-4702-b376-2dacce773dc0&amp;DisplayLang=en</a></li> <li>3. Double-click the Hot Fix to run.</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>
<b>DocuColor 3535 with EFI Network Controller</b>	<p>DocuColor 3535 with EFI Network Controller is Linux-based and is not, therefore, affected by this vulnerability.</p>
<b>DocuColor Windows NT based products with EFI front-ends:</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> </ul>	<p>These DocuColor products with EFI front-ends are affected by this vulnerability. Patch 1-AX671 can be downloaded from Xerox Technical Support at <a href="http://www.xerox-techsupport.com/">http://www.xerox-techsupport.com/</a>. To find the patch, search for Patch 1-AX671 or select the appropriate product and configuration and navigate to the patch.</p>
<b>DocuColor Windows XPe based products with EFI front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 3535 with EX3535</li> </ul>	<p>DocuColor Windows XPe based products with EFI front-ends are affected by this vulnerability. Patch 1-DSRD9 can be downloaded from the 'Critical Security Updates' section of the <a href="#">DocuColor 3535's Drivers and Downloads</a> page.</p>
<b>DocuColor with Creo front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 3535 with CXP3535</li> <li>• DocuColor 6060/2060 with CXP6000</li> </ul>	<p>DocuColor 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/downloads/details.aspx?FamilyId=F4F66D56-E7CE-44C3-8B94-817EA8485DD1&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?FamilyId=F4F66D56-E7CE-44C3-8B94-817EA8485DD1&amp;displaylang=en</a></li> <li>3. Double-click the Hot Fix to run.</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>
<b>DocuColor with EFI Splash front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 3535 with G3535</li> <li>• DocuColor 12 with G640</li> </ul>	<p>DocuColor products with EFI Splash front-ends are Macintosh-based and are not, therefore, affected by this vulnerability.</p>

Product	Response to <a href="#">CERT Advisory CA-2003-23</a>
<b>Document Centre products (200, 300, 400 and 500 Series)</b>	Document Centre products do not include the Windows Operating System and are not, therefore, affected by this advisory.
<b>DocuPrint N Series products</b>	DocuPrint N Series products do not include the Windows Operating System and are not, therefore, affected by this advisory.
<b>DocuPrint NPS/IPS Series products</b>	DocuPrint NPS/IPS Series products are not based on Microsoft software and are not, therefore, affected by this advisory.
<b>DocuSP-based products</b>	DocuSP-based products are Sun Solaris based and are not, therefore, affected by this advisory.
<b>iGen3 Creo Spire Color Controller</b>	<p>The iGen3 Creo Spire Color Controller is 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/downloads/details.aspx?FamilyId=F4F66D56-E7CE-44C3-8B94-817EA8485DD1&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?FamilyId=F4F66D56-E7CE-44C3-8B94-817EA8485DD1&amp;displaylang=en</a></li> <li>3. Double-click the Hot Fix to run.</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>
<b>Phaser products</b>	Phaser products do not include the Windows Operating System and are not, therefore, affected by this advisory.
<b>WorkCentre M35</b> <b>WorkCentre M45</b> <b>WorkCentre M55</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 32 Color</b> <b>WorkCentre Pro 40 Color</b>	These WorkCentre products do not include the Windows Operating System and are not, therefore, affected by this advisory.
<b>Xerox 2101</b>	The Xerox 2101 is affected by this vulnerability. Patch 1-DSRD9 can be downloaded from the 'Critical Security Updates' section of the <a href="#">Xerox 2101's Drivers and Downloads</a> page.

**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.