

## Xerox Product Response to US-CERT® Technical Cyber Security Alert TA04-217A: Multiple Vulnerabilities in libpng (MS05-009)

### 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 TA04-217A](#), issued by US-CERT® on August 4<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 TA04-217A](#) describes several vulnerabilities that exist in the libpng library, the most serious of which could allow a remote attacker to execute arbitrary code on an affected 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 <a href="#">US-CERT® Technical Cyber Security Alert TA04- 217A</a>
<b>FreeFlow Makeready, Process Manager, and Web Services (includes DigiPath)</b>	FreeFlow Makeready, Process Manager, and Web Services (including DigiPath) does not use the libpng library and is not, therefore, affected by this vulnerability.
<b>DocuColor 1632/2240</b>	The DocuColor 1632/2240 products do not contain or use the libpng library and are not, therefore, affected by this vulnerability.
<b>DocuColor 3535 with EFI Network Controller</b>	The DocuColor 3535 with EFI Network Controller is Linux-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 affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative. <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/MS05-009.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-009.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>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 217A</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 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/MS05-009.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-009.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 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/MS05-009.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-009.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 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/MS05-009.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-009.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 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 with EFI Splash front-ends are Macintosh 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 do not contain or use the libpng library and are not, therefore, affected by this vulnerability.</p>
<p><b>DocuPrint N Series products</b></p>	<p>DocuPrint N Series Products do not use libpng and are not, therefore, affected by this vulnerability.</p>
<p><b>DocuPrint NPS/IPS Series products</b></p>	<p>DocuPrint NPS/IPS Series products do not use the libpng library and are not, therefore, affected by this vulnerability.</p>

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 217A</a>
<b>DocuSP-based products</b>	DocuSP-based products do not use the libpng library and are not, therefore, affected by this vulnerability.
<b>Phaser products</b>	Phaser products do not support the libpng library and are not, therefore, affected by this vulnerability.
<b>WorkCentre M24</b> <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 contain or use the libpng library and are 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 and 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.

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA04- 217A</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 and FACI are not affected by this vulnerability.</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 not affected by this vulnerability.</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.