

Xerox Product Response to US-CERT® Technical Cyber Security Alert TA04-260A: Microsoft Windows JPEG component buffer overflow (MS04-028)

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 TA04-260A](#), issued by US-CERT® on September 16th, 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 (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 TA04-260A](#) states that Microsoft's Graphic Device Interface Plus (GDI+) contains a vulnerability in the processing of JPEG images. This vulnerability may allow attackers to remotely execute arbitrary code on the affected system. Exploitation may occur as the result of viewing a malicious web site, reading an HTML-rendered email message, or opening a crafted JPEG image in any vulnerable application. The privileges gained by a remote attacker depend on the software component being attacked.

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 US-CERT® Technical Cyber Security Alert TA04- 260A
CopyCentre C20	The CopyCentre C20 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.

Product	Response to US-CERT® Technical Cyber Security Alert TA04- 260A
<p>DigiPath</p>	<p>DigiPath is affected by this vulnerability. DigiPath 3.0/4.x customers should use the following instructions to update your DigiPath system:</p> <p><u>Instructions for using Windows Update on DigiPath version 3.0/4.x</u></p> <ol style="list-style-type: none"> 1. Ensure that a TapeWare system backup exists. 2. On a weekly basis, run Windows Update: <p>Note: Operating System and Internet Explorer Service Packs are not 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 “Install Now”.</p> <ol style="list-style-type: none"> a. Log in to the system as DPAdmin. b. Run the xstopdgp.bat file to cycle down the DigiPath software. Select [Start:Run], then enter e:\digipath\xstopdgp.bat in the window. c. Open Internet Explorer and select “Windows Update” from the Tools menu -or- select “Windows Update” from your Windows Start Menu. d. If prompted to install the latest Windows Update software, select [Yes]. Then select [Yes] to reboot your machine. If you did not receive this prompt, proceed to step f. e. Once your system has rebooted, return back to step ‘a’ to continue. f. Select “Scan for Updates” in the main center window. g. In the left window pane, select “Critical Updates and Service Packs”. h. Select “Review and Install Updates”. See Note above regarding de-selection of Service Packs. i. Select [Install Now] to download all the Microsoft critical updates needed for your system. j. Select [Accept] to accept the Microsoft license agreement. k. The patches will be downloaded and installed. <p>If prompted, select [Yes] to restart your system.</p>
<p>DocuColor 1632/2240</p>	<p>The DocuColor 1632/2240 products are not Microsoft Windows-based and are not, therefore, affected by this vulnerability.</p>
<p>DocuColor 3535 with EFI Network Controller</p>	<p>The DocuColor 3535 with EFI Network Controller is Linux-based and is, therefore, not affected by this vulnerability.</p>
<p>DocuColor Windows 2000 based products with Creo front-ends:</p> <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535 • DocuColor 6060/5252/2060/2045 with CXP6000 • DocuColor 5252/2045 with CXP5000 	<p>DocuColor Windows 2000 based products with Creo front-ends are not affected by this vulnerability.</p>
<p>DocuColor Windows NT based products with Creo front-ends:</p> <ul style="list-style-type: none"> • DocuColor 2060/2045 with CSX2000 	<p>DocuColor Windows NT based products with Creo front-ends are not affected by this vulnerability.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA04- 260A
<p>DocuColor Windows XP Professional SP1 based products with Creo front-ends:</p> <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535e 	<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><u>Patch installation instructions:</u></p> <ol style="list-style-type: none"> 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-028.msp 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
<p>DocuColor Windows XP Professional SP2 based products with Creo front-ends:</p> <ul style="list-style-type: none"> ▪ DocuColor 3535 with CXP3535e 	<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>DocuColor Windows NT based products with EFI front-ends and Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 12 with X12 • DocuColor 12 with EX12 • DocuColor 12 with XP12 • DocuColor 40 with X40 • DocuColor 2045/2060 with EX2000 • DocuColor 2045/2060/5252 with EX2000d • DocuColor 2045/2060 with EX2000v 	<p>DocuColor Windows NT based products with EFI front-ends and FACI do not contain or support the GDI+ library and are not, therefore, affected by this vulnerability.</p>
<p>DocuColor Windows NT based products with EFI front-ends without the Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 12 with X12 • DocuColor 12 with EX12 • DocuColor 12 with XP12 • DocuColor 40 with X40 	<p>DocuColor Windows NT based products with EFI front-ends without FACI do not contain or support the GDI+ library and are not, therefore, affected by this vulnerability.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA04- 260A
<p>DocuColor Windows XPe based products with EFI front-ends and Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 3535 with EX3535 • DocuColor 5252 with EXP5000 • DocuColor 6060 with EXP6000 • DocuColor 8000 with EXP8000 	<p>DocuColor Windows XPe based products with EFI front-ends and FACI do not contain or support the GDI+ library and are not, therefore, affected by this vulnerability.</p>
<p>DocuColor Windows XPe based products with EFI front-ends <u>without</u> the Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 3535 with EX3535 	<p>DocuColor Windows XPe based products with EFI front-ends without FACI do not contain or support the GDI+ library and are not, therefore, affected by this vulnerability.</p>
<p>DocuColor with EFI Splash front-ends:</p> <ul style="list-style-type: none"> • DocuColor 12 with G640 • DocuColor 3535 with G3535 	<p>DocuColor products with EFI Splash are Macintosh-based and are not, therefore, affected by this vulnerability.</p>
<p>Document Centre products (200, 300, 400 and 500 Series)</p>	<p>Document Centre products do not contain or use the GDI+ library and are not, therefore, affected by this vulnerability.</p>
<p>DocuPrint N Series products</p>	<p>DocuPrint N Series products do not contain or use the GDI+ library and are not, therefore, affected by this vulnerability.</p>
<p>DocuPrint NPS/IPS Series products</p>	<p>DocuPrint NPS/IPS Series products are Sun-based and are not, therefore, affected by this vulnerability.</p>
<p>DocuSP-based products</p>	<p>DocuSP-based products are Sun Solaris-based and are not, therefore, affected by this vulnerability.</p>
<p>FaxCentre F12</p>	<p>The FaxCentre F12 is not Microsoft Windows-based and is not, therefore, affected by this vulnerability.</p>
<p>Phaser products</p>	<p>Phaser products do not contain or use the GDI+ library and are not, therefore, affected by this vulnerability.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA04- 260A
WorkCentre M15 WorkCentre M20/M20i WorkCentre M24 WorkCentre M35 WorkCentre M45 WorkCentre M55 WorkCentre PE16 WorkCentre Pro 35 WorkCentre Pro 45 WorkCentre Pro 55 WorkCentre Pro 65 WorkCentre Pro 75 WorkCentre Pro 90 WorkCentre Pro 423 WorkCentre Pro 428 WorkCentre Pro 32 Color WorkCentre Pro 40 Color	These WorkCentre products do not contain or use the GDI+ library and are not, therefore, 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.