

Xerox Product Response to US-CERT® Technical Cyber Security Alert TA05-312A: Microsoft Windows Image Processing Vulnerabilities (MS05-053)

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 TA05-312A](#), issued by US-CERT® on November 8th, 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® Technical Cyber Security Alert TA05-312A](#) states that Microsoft has released updates that address critical vulnerabilities in Windows graphics rendering services. A remote, unauthenticated attacker exploiting these vulnerabilities could execute arbitrary code or cause a denial of service 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 US-CERT® Technical Cyber Security Alert TA05-312A
CentreWare Network Scanning Services	CentreWare Network Scanning Services is not directly affected by these vulnerabilities. Operating systems on which CentreWare Network Scanning Services reside may be affected. We recommend that our customers install the latest operating system security patches.
CentreWare Network Services	CentreWare Network Services is not directly affected by these vulnerabilities. Operating systems on which CentreWare Network Services reside may be affected. We recommend that our customers install the latest operating system security patches.
CopyCentre C20 CopyCentre C123 CopyCentre C128	These CopyCentre products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.
DocuColor 2240/1632	The DocuColor 2240/1632 is not Microsoft Windows-based and is not, therefore, affected by these vulnerabilities.
DocuColor 3535 with EFI Network Controller	DocuColor 3535 with EFI Network Controller is not Microsoft Windows-based and is not, therefore, affected by these vulnerabilities.
DocuColor with EFI Splash front-ends: <ul style="list-style-type: none"> • DocuColor 12 with G640 • DocuColor 3535 with G3535 	DocuColor products with EFI Splash front-ends are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.

Product	Response to US-CERT® Technical Cyber Security Alert TA05-312A
Document Centre Xerox WIA Driver for Microsoft® Windows XP®	Document Centre Xerox WIA Driver for Microsoft Windows XP is not directly affected by these vulnerabilities. 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.
DocuPrint N Series products	DocuPrint N Series products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products are Sun-based and are not, therefore, affected by these vulnerabilities.
DocuSP-based products	DocuSP-based products are Sun Solaris-based and are not, therefore, affected by these vulnerabilities.
FaxCentre F12	The FaxCentre F12 is not Microsoft Windows-based and is not, therefore, affected by these vulnerabilities.
FlowPort	FlowPort is not directly affected by these vulnerabilities. Operating systems on which Flowport resides may be affected. We recommend that our customers install the latest operating system security patches.
FreeFlow Makeready, Process Manager, and Web Services (includes DigiPath)	FreeFlow Makeready, Process Manager, and Web Services including DigiPath are not directly affected by these vulnerabilities. Operating systems on which they reside may be affected. We recommend that our customers install the latest operating system security patches using Microsoft Update.
FreeFlow SMARTsend™	FreeFlow SMARTsend™ is not directly affected by these vulnerabilities. Operating systems on which SMARTsend resides may be affected. We recommend that our customers install the latest operating system security patches.
Phaser products	Phaser products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.

Product	Response to US-CERT® Technical Cyber Security Alert TA05-312A
<p> WorkCentre M15 WorkCentre M20/M20i WorkCentre M24 WorkCentre M35 WorkCentre M45 WorkCentre M55 WorkCentre M123 WorkCentre M128 WorkCentre PE16 WorkCentre Pro 35 WorkCentre Pro 45 WorkCentre Pro 55 WorkCentre Pro 65 WorkCentre Pro 75 WorkCentre Pro 90 WorkCentre Pro 123 WorkCentre Pro 128 WorkCentre Pro 423 WorkCentre Pro 428 WorkCentre Pro 32 Color WorkCentre Pro 40 Color WorkCentre Pro C2128 WorkCentre Pro C2636 WorkCentre Pro C3545 </p>	<p>These WorkCentre products are not Microsoft Windows-based and are not, therefore, affected by these vulnerabilities.</p>
<p>Xerox 1010/2101 Windows NT Copy Server</p>	<p>The Xerox 1010/2101 Windows NT Copy Server is not affected by this vulnerability.</p>
<p>Xerox products with EFI Windows XPe based front ends with Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 12 with X12/EX12/XP12 (customer purchased s/w option) • DocuColor 3535 with EX3535 • DocuColor 5252 with EXP5000 • DocuColor 6060 with EXP6000 • DocuColor 8000 with EXP8000 • Phaser EX7750 • Xerox 2101 with EX2101 	<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 --> All Program --> System Update</p> <p style="text-align: center;">-----</p> <p>* DocuColor 3535 with EX3535 v1.0: System Update is available after the appropriate patch has been installed. The Systems Updates Patch can be found at http://www.support.xerox.com/go/getfile.asp?Xlang=en_US&XCntry=USA&objid=44488&EULA=0&prodId=DC_3535&Family=DocuColor&ripld=XRIP_Fiery_EX3535&langs=English%20(US)&plats=Windows%20XP&Xtype=download.</p> <p>When the System Updates Patch has been successfully installed, follow the detailed instructions above.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA05-312A
<p>Xerox products with EFI Windows XPe based front ends <u>without</u> Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none">• DocuColor 12 with X12/EX12/XP12 (customer purchased s/w option)• DocuColor 3535 with EX3535• Phaser EX7750• Xerox 2101 with EX2101	<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.