

Xerox Product Response to CERT[®] Advisories**CA-2003-16: Buffer Overflow in Microsoft RPC (MS03-026)****CA-2003-19: Exploitation of Vulnerabilities in Microsoft RPC Interface
(MS03-026)****CA-2003-20: W32/Blaster worm (MS03-026)****Audience and Purpose**

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [CERT[®] Advisory CA-2003-16](#), [CERT[®] Advisory CA-2003-19](#), and [CERT[®] Advisory CA-2003-20](#) issued by CERT[®]. The following sections provide excerpts from the CERT[®] advisories and the corresponding Xerox response.

Background

The CERT[®] 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[®] 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.

All vulnerabilities listed above are related to the same Microsoft Windows[®] vulnerability. The vulnerability is a buffer overflow that exists in Microsoft's Remote Procedure Call (RPC) implementation. A remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

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 CERT[®] Advisory CA-2003-16 , CERT[®] Advisory CA-2003-19 , CERT[®] Advisory CA-2003-20
DigiPath	DigiPath products are affected by this vulnerability. The Microsoft patch available to address this vulnerability is captured in the following Xerox security bulletins: #153 for DigiPath 2.1 and #154 for DigiPath 3.0. Please contact your Xerox Representative for more information.
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 Mac OS based and are not, therefore, affected by this vulnerability.
DocuColor 2060/2045 with CSX2000	The DocuColor 2060/2045 with CSX2000 is affected by this vulnerability. A patch to address this vulnerability is available from http://www.xerox-techsupport.com/dc2000/DC6060/CXP6000_Patches/CXP6000_NT_Win2K_M_SBlaster.htm .
DocuColor 3535 with EFI Network Controller	DocuColor 3535 with EFI Network Controller is Linux based and is not, therefore, affected by this vulnerability.

Product	Response to CERT[®] Advisory CA-2003-16 , CERT[®] Advisory CA-2003-19 , CERT[®] Advisory CA-2003-20
DocuColor 6060/2060 with CXP6000	The DocuColor 6060/2060 with CXP6000 is affected by this vulnerability. A patch to address this vulnerability is available from http://www.xerox-techsupport.com/dc2000/DC6060/CXP6000_Patches/CXP6000_NT_Win2K_M_SBlaster.htm .
DocuColor Windows XPe based products with EFI front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with EX3535 	DocuColor Windows XPe based products with EFI front-ends include the patch for this vulnerability and are not, therefore, affected by this vulnerability.
DocuColor with EFI Front ends: <ul style="list-style-type: none"> • DocuColor 12 with X12 • DocuColor 12 with XP12 • DocuColor 12 with EX12 • DocuColor 2045/2060 with EX2000 • DocuColor 2045/2060 with EX2000D • DocuColor 2045/2060 with EX2000v • DocuColor 6060 with EXP6000 	DocuColor products with EFI front-ends are affected by this vulnerability. Patch 1-ANC11 can be downloaded from Xerox Technical Support at http://www.xerox-techsupport.com/ . To find the patch, search for Patch 1-ANC11 or select the appropriate product and configuration and navigate to the patch.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products do not include the Windows Operating System and are not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products do not include the Windows Operating System and are not, therefore, affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products are not based on Microsoft software and are not, therefore, affected by this vulnerability.
DocuSP-based products	DocuSP-based products are Sun Solaris based and are not, therefore, affected by this vulnerability.
iGen3 Creo Spire Color Controller	<p>The iGen3 Creo Spire Color Controller is affected by this vulnerability. Please use the following instructions to update your system, or you may 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/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en 3. Double-click the Hot Fix to run. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.

Product	Response to CERT[®] Advisory CA-2003-16 , CERT[®] Advisory CA-2003-19 , CERT[®] Advisory CA-2003-20
Phaser products	Phaser products do not include the Windows Operating System and are not, therefore, affected by this vulnerability.
WorkCentre M35 WorkCentre M45 WorkCentre M55 WorkCentre Pro 35 WorkCentre Pro 45 WorkCentre Pro 55 WorkCentre Pro 65 WorkCentre Pro 75 WorkCentre Pro 90 WorkCentre Pro 32 Color WorkCentre Pro 40 Color	These WorkCentre products do not include the Windows Operating System 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.