

Xerox Product Response to CERT® Advisory CA-2004-01 and CERT Vulnerability Note VU#749342: *Multiple H.323 Message Vulnerabilities (MS04-001)*

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-2004-01](#) and [CERT® Vulnerability Note VU# 749342](#) 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.

The vulnerabilities listed above report the same H.323 vulnerability. They describe multiple vulnerabilities in different vendor implementations of the multimedia telephony protocols H.323 and H.225. H.323 and H.225 are international standard protocols, published by the International Telecommunications Union and used to facilitate communication among telephony and multimedia systems.

Xerox Product Response

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

Product	Response to CERT Advisory CA-2004-01 , CERT Vulnerability Note VU# 749342
CentreWare Network Scanning Services	CentreWare Network Scanning Services does not use the H.323 protocol and is not, therefore, affected by this vulnerability.
CentreWare Network Services	CentreWare Network Services does not use the H.323 protocol and is not, therefore, affected by this vulnerability.
DigiPath	DigiPath products do not use the H.323 protocol and are not, therefore, affected by this vulnerability.
DocuColor 1632/2240	The DocuColor 1632/2240 products do not use the H.323 protocol and are not, therefore, affected by this vulnerability
DocuColor 3535 with EFI Network Controller	The DocuColor 3535 with EFI Network Controller does not use the H.323 protocol and is not, therefore, affected by this vulnerability
DocuColor Windows 2000 based products with Creo front-ends: <ul style="list-style-type: none">• DocuColor 3535 with CXP3535• DocuColor 6060/5252/2060/2045 with CXP6000• DocuColor 5252/2045 with CXP5000• DC3535 with CXP3535	DocuColor Windows 2000 based products with Creo front-ends are not affected by this vulnerability.

Product	Response to CERT Advisory CA-2004-01 , CERT Vulnerability Note VU# 749342
DocuColor Windows NT based products with Creo front-ends: <ul style="list-style-type: none"> ▪ DocuColor 2060/2045 with CSX2000 	DocuColor Windows NT based products with Creo front-ends are not affected by this vulnerability.
DocuColor Windows XP Professional SP1 based products with Creo front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535e 	DocuColor Windows XP Professional SP1 based products with Creo front-ends are not affected by this vulnerability.
DocuColor Windows XP Professional SP2 based products with Creo front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535e 	DocuColor Windows XP Professional SP2 based products with Creo front-ends are not affected by this vulnerability.
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 do not use the H.323 protocol and are not, therefore, affected by this vulnerability.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products do not use the H.323 protocol and are not, therefore, affected by this vulnerability.
Document Centre Xerox WIA Driver for Microsoft® Windows XP®	The Document Centre Xerox WIA Driver for Microsoft® Windows XP® does not use the H.323 protocol and is not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products do not use the H.323 protocol and are not, therefore, affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products do not use the H.323 protocol 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.
Flowport	Flowport does not use the H.323 protocol and is not, therefore, affected by this vulnerability.
Phaser products	Phaser products do not use the H.323 protocol and are not, therefore, affected by this vulnerability.
WorkCentre M24	WorkCentre M24 does not use the H.323 protocol and is not, therefore, affected by this vulnerability.

Product	Response to CERT Advisory CA-2004-01 , CERT Vulnerability Note VU# 749342
<p>WorkCentre M35 WorkCentre M45 WorkCentre M55</p> <p>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</p>	<p>These WorkCentre products do not use the H.323 protocol and are not, therefore, affected by this vulnerability.</p>
<p>Xerox products with EFI Windows NT based front ends with 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 • Xerox 1010 with EX1010 	<p>Xerox products with EFI Windows NT based front ends with FACI do not use the H.323 protocol and are not, therefore, affected by this vulnerability.</p>
<p>Xerox products with EFI Windows NT based front ends <u>without</u> 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 • Xerox 1010 with EX1010 	<p>Xerox products with EFI Windows NT based front ends without FACI do not use the H.323 protocol and are not, therefore, affected by this vulnerability.</p>

Product	Response to CERT Advisory CA-2004-01 , CERT Vulnerability Note VU# 749342
<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 do not use the H.323 protocol and are not, therefore, affected by this vulnerability.</p>
<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 do not use the H.323 protocol and are not, therefore, 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.