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 these vulnerabilities. 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.
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.

Product	Response to CERT Advisory CA-2004-01, CERT Vulnerability Note VU# 749342
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 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 use the H.323 protocol 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 no allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.