Xerox Product Response to CERT® Vulnerability Note VU#383779: *ZIP archives containing files with large filenames can cause buffer overflows (MS02-054)*

Audience and Purpose

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to CERT® Vulnerability Note VU#383779, issued by CERT® on October 2nd, 2002. The following sections provide excerpts from the CERT® advisory 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.

CERT® Vulnerability Note VU#383779 refers to a vulnerability in several ZIP archive utilities. The vulnerability states that ZIP archives containing files with large filenames can be used to trigger heap and stack buffer overflows in several file decompression utilities.

Xerox Product Response

The table below lists various products and their positions with respect to CERT® Vulnerability Note VU#383779. This document will be updated with additional product information as it becomes available.

Product	Response to CERT® Vulnerability Note VU#383779
CentreWare Network Scanning Services	CentreWare Network Scanning Services does not use the ZIP utilities and is not, therefore, affected by this vulnerability.
CentreWare Network Services	CentreWare Network Services does not use the ZIP utilities and is not, therefore, affected by this vulnerability.
DigiPath	DigiPath does not require the use of ZIP utilities and is not, therefore, affected by this vulnerability.
DocuColor 1632/2240	DocuColor 1632/2240 products do not use ZIP archives 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 ZIP utilities and is not, therefore, affected by this vulnerability.
DocuColor with CREO front-ends: • **DocuColor 2060/2045 with CSX2000** • **DocuColor 3535 with CXP3535** • **DocuColor 6060/2060 with CXP6000**	DocuColor products with CREO front-ends do use ZIP utilities and are not, therefore, affected by this vulnerability.

Product	Response to CERT® Vulnerability Note VU#383779
DocuColor Windows NT based products with EFI front-ends: • **DocuColor 12 with X12** • **DocuColor 12 with EX12** • **DocuColor 12 with XP12** • **DocuColor 40 with X40** • **DocuColor 2045/2060 with EX2000** • **DocuColor 2045/2060 with EX2000d** • **DocuColor 2045/2060 with EX2000v** • **DocuColor 6060 with EXP6000**	DocuColor Windows NT based products with EFI front-ends are not affected by this vulnerability.
DocuColor Windows XPe based products with EFI front-ends: • **DocuColor 3535 with EX3535**	DocuColor Windows XPe based products with EFI front-ends are Microsoft Windows based and are not, therefore, affected by this vulnerability.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products do not execute any ZIP utilities and are not, therefore, affected by this vulnerability.
Document Centre Xerox WIA Driver for Microsoft® Windows XP®	Document Centre Xerox WIA Driver for Microsoft® Windows XP® does not use the ZIP utilities and is not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products do not execute any ZIP utilities. DocuPrint does supply some software and files using the self-extracting .EXE files, which are generated by the WinRAR utility that has been determined to be safe according to CERT® VU#383779.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products do not use ZIP archives and are not, therefore, affected by this vulnerability.
DocuSP-based products	DocuSP-based products are Sun® (Solaris™)-based and do not execute any ZIP utilities; they are not, therefore, affected by this vulnerability.
Phaser products	Phaser products do not execute any ZIP utilities. They do supply some software and files using the self-extracting .EXE files, which are generated by the WinRAR utility that has been determined to be safe according to CERT® VU#383779.

Product	Response to CERT® Vulnerability Note VU#383779
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 execute any ZIP utilities 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.