Xerox Product Response to CERT® Vulnerability Note VU#192995*: Integer overflow in xdr_array() function when deserializing the XDR stream*

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#192995, issued by CERT® on July 31st, 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#192995 refers to an integer overflow present in the *xdr_array()* function in the XDR library provided by Sun Microsystems. This overflow has been shown to lead to remotely exploitable buffer overflows in multiple applications, leading to the execution of arbitrary code.

Xerox Product Response

The table below lists various products and their positions with respect to CERT® Vulnerability Note VU#192995. This document will be updated with additional product information as it becomes available.

Product	Response to CERT® Vulnerability Note VU#192995
DigiPath	DigiPath does not use the Unix 3.0 Interix SDK and is not, therefore, affected by this vulnerability.
DocuColor with CREO Front ends: • **DocuColor 2045/2060(xx) with CSX2000** • **DocuColor 6060(xx) with CXP6000**	DocuColor products with CREO front ends are not affected by this vulnerability.
DocuColor with EFI Front ends : • **DocuColor 2045/2060(xx) with (EX2000/EX2000D/EX2000v)** • **DocuColor 6060(xx) with EXP6000** • **DocuColor 12(xx) with (X12/XP12/EX12)**	DocuColor products with EFI front ends are not affected by this vulnerability.
Document Centre products	Document Centre products do not use Sun® RPC and are not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products are not sold with Sun® workstations or software, and are not, therefore, affected by this vulnerability.
DocuSP-based products	DocuSP-based products are affected by this vulnerability. Patches are in process and will be announced when available.
Phaser products	Phaser products are not sold with Sun® workstations or software, and are not, therefore, affected by this vulnerability.

THE DOCUMENT COMPANY
XEROX®

Product	Response to CERT® Vulnerability Note VU#192995
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 Pro products do not use Sun® RPC 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.