Xerox Product Response to CERT® Vulnerability Note VU# 412115: *Network device drivers reuse old frame buffer data to pad packets*

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# 412115, issued by CERT® on January 6th, '2003. 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#412115 states that many Ethernet device drivers fail to pad frames with null bytes. Instead, these device drivers reuse previously transmitted frame data to pad frames smaller than 46 bytes. This constitutes an information leakage vulnerability that may allow remote attackers to harvest potentially sensitive information.

Xerox Product Response

The table below lists various products and their positions with respect to CERT® Vulnerability Note VU#412115. This document will be updated with additional product information as it becomes available.

Product	Response to CERT® Vulnerability Note VU#412115
DigiPath	DigiPath does not provide any Ethernet drivers on top of what Microsoft Corporation provides. Microsoft Corporation states they are not vulnerable; therefore, DigiPath is not affected by this vulnerability.
DocuColor 1632/240	DocuColor 1632/2240 products are affected by this vulnerability. The vulnerability will be fixed in an upcoming maintenance release.
DocuColor 3535 with EFI Network Controller	The DocuColor 3535 with EFI Network Controller is not 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 are not affected by this vulnerability.

Product	Response to CERT® Vulnerability Note VU#412115
DocuColor Windows NT based products with EFI front-ends: • **DocuColor 12 with X12** • **DocuColor 12 with EX12** • **DocuColor 12 with XP12** • **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 not affected by this vulnerability.
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 utilize the network devices, or operating systems listed in this vulnerability and are not susceptible.
DocuPrint N Series products	DocuPrint N Series products are not vulnerable since the embedded products zero pad bytes when constructing the packets.
DocuSP-based products	DocuSP-based products are not affected by this vulnerability.
Phaser products	Phaser products are not vulnerable since the embedded products zero pad bytes when constructing the packets.
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 utilize the network devices, or operating systems listed in this vulnerability and are not susceptible.

Contact

For additional information or clarification on any of the product information given here, contact Xerox support.

Disclaimer