

Xerox Product Response to US-CERT® Technical Cyber Security Alert TA04-111A: Vulnerabilities in TCP

Audience and Purpose

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [US-CERT® Technical Cyber Security Alert TA04-111A](#), issued by US-CERT® on April 20th, 2004. The following sections provide excerpts from the US-CERT® Technical Cyber Security Alert and the corresponding Xerox response.

Background

The [United States-Computer Emergency Readiness Team](#) (US-CERT) is a partnership between the National Cyber Security Division (NCSD) at the [Department of Homeland Security](#) (DHS) and the private sector. US-CERT provides individuals and organizations with access to valuable educational resources as well as up-to-date computer security information via the [National Cyber Alert System](#).

[US-CERT® Technical Cyber Security Alert TA04-111A](#) describes a vulnerability in TCP which allows remote attackers to terminate network sessions. Sustained exploitation of this vulnerability could lead to a denial of service condition.

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 US-CERT® Technical Cyber Security Alert TA04-111A
CentreWare Network Scanning Services	CentreWare Network Scanning Services does not support BGP and is not, therefore, affected by this vulnerability.
CentreWare Network Services	CentreWare Network Services does not support BGP and is not, therefore, affected by this vulnerability.
DigiPath	DigiPath does not support BGP and is not, therefore, affected by this vulnerability.
DocuColor 1632/2240	The DocuColor 1632/2240 products do not support BGP and are not, therefore, affected by this vulnerability.
DocuColor 3535 with EFI Network Controller	The DocuColor 3535 with EFI Network Controller does not support persistent TCP connections 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 	DocuColor Windows 2000 based products with Creo front-ends do not support BGP and are not, therefore, affected by this vulnerability.

Product	Response to US-CERT® Technical Cyber Security Alert TA04-111A
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 do not support BGP and are not, therefore, 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 do not support BGP and are not, therefore, 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 do not support BGP and are not, therefore, 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 support persistent TCP connections and are not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products do not support BGP and are not, therefore, affected by this vulnerability.
FaxCentre F12	The FaxCentre F12 does not support BGP and is not, therefore affected by this vulnerability.
FlowPort	FlowPort does not support BGP and is not, therefore, affected by this vulnerability.
FreeFlow Makeready, Process Manager, and Web Services (includes DigiPath)	FreeFlow Makeready, Process Manager, and Web Services (including DigiPath) do not support persistent TCP connections and are not, therefore, affected by this vulnerability.
FreeFlow SMARTsend	FreeFlow SMARTsend does not support BGP and is not, therefore, affected by this vulnerability.
iGen3 Windows 2000-based Creo Spire Color Server	The iGen3 Windows 2000-based Creo Spire Color Server does not support BGP and is not, therefore, affected by this vulnerability.
Phaser products	Phaser products do not support BGP and are not, therefore, affected by this vulnerability.

Product	Response to US-CERT® Technical Cyber Security Alert TA04-111A
<p>WorkCentre M15 WorkCentre M24 WorkCentre M35 WorkCentre M45 WorkCentre M55</p> <p>WorkCentre PE16</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 WorkCentre Pro 423 WorkCentre Pro 428</p>	<p>These WorkCentre products do not support BGP 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 support persistent TCP connections 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 support persistent TCP connections and are not, therefore, affected by this vulnerability.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA04-111A
<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 support persistent TCP connections 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 support persistent TCP connections 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.