

Xerox Product Response to CERT[®] Advisory CA-2002-28 Trojan Horse Sendmail Distribution

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-2002-28](#), issued by CERT[®] on October 8th, 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[®] Advisory CA-2002-28](#) refers to a vulnerability in some copies of the source code for the Sendmail package that have been modified by an intruder to contain a Trojan horse. These files began to appear in downloads from the FTP server ftp.sendmail.org on or around September 28, 2002. The Sendmail development team disabled the compromised FTP server on October 6, 2002 at approximately 22:15 PDT. An intruder operating from the remote address specified in the malicious code can gain unauthorized remote access to any host that compiled a version of Sendmail from this Trojan horse version of the source code. The level of access would be that of the user who compiled the source code.

Xerox Product Response

The table below lists various products and their positions with respect to [CERT[®] Advisory CA-2002-28](#). The table will be updated with product information as it becomes available.

Product	Response to CERT[®] Advisory CA-2002-28
CentreWare Network Scanning Services	CentreWare Network Scanning Services does not use Sendmail and is not, therefore, affected by this vulnerability.
CentreWare Network Services	CentreWare Network Services does not use Sendmail and is not, therefore, affected by this vulnerability.
DigiPath	DigiPath is not affected by this vulnerability.
DocuColor 1632/2240	The DocuColor 1632/2240 products are not affected by this vulnerability.
DocuColor with CREO front-ends: <ul style="list-style-type: none"> • DocuColor 2060/2045 with CSX2000 • DocuColor 3535 with CXP3535 • DocuColor 6060/2060 with CXP6000 	DocuColor products with CREO front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.

Product	Response to CERT® Advisory CA-2002-28
DocuColor Windows NT based products with EFI front-ends: <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 with EX2000d • DocuColor 2045/2060 with EX2000v • DocuColor 6060 with EXP6000 	DocuColor Windows NT based products with EFI front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.
DocuColor Windows XPe based products with EFI front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with EX3535 	DocuColor Windows XPe based products with EFI front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.
DocuColor 3535 with EFI Network Controller	The DocuColor 3535 with EFI Network Controller does not use Sendmail and is 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 use Sendmail and are not, therefore, affected by this vulnerability.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products do not use Sendmail and are not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products do not use Sendmail and are not, therefore, affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products do not use Sendmail and are not, therefore, affected by this vulnerability.
Phaser products	Phaser products do not use Sendmail and are not, therefore, affected by this vulnerability.

Product	Response to CERT® Advisory CA-2002-28
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 Sendmail 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 not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.