

## Xerox Product Response to CERT<sup>®</sup> Advisory CA-2003-12: *Buffer Overflow in Sendmail*

### Audience and Purpose

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [CERT<sup>®</sup> Advisory CA-2003-12](#), issued by CERT<sup>®</sup> on March 29<sup>th</sup>, 2003. The following sections provide excerpts from the CERT<sup>®</sup> advisory and the corresponding Xerox response.

### Background

The CERT<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> Advisory CA-2003-12](#) describes a vulnerability in Sendmail that can be exploited to cause a denial-of-service condition and could allow a remote attacker to execute arbitrary code with the privileges of the Sendmail daemon, typically root.

### Xerox Product Response

The table below lists various products and their positions with respect to [CERT<sup>®</sup> Advisory CA-2003-12](#). The table will be updated with product information as it becomes available.

Product	Response to <a href="#">CERT<sup>®</sup> Advisory CA-2003-12</a>
<b>CentreWare Network Scanning Services</b>	CentreWare Network Scanning Services does not use Sendmail and is not, therefore, affected by this vulnerability.
<b>CentreWare Network Services</b>	CentreWare Network Services does not use Sendmail and is not, therefore, affected by this vulnerability.
<b>DigiPath</b>	DigiPath is not impacted by this vulnerability.
<b>DocuColor 1632/2240</b>	The DocuColor 2240/1632 products do not use Sendmail and are not, therefore, affected by this vulnerability.
<b>DocuColor 3535 with EFI Network Controller</b>	DocuColor 3535 with EFI Network Controller does not use Sendmail and is not, therefore, affected by this vulnerability.
<b>DocuColor with CREO Front ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 2060/2045 with CSX2000</li> <li>• DocuColor 3535 with CXP3535</li> <li>• DocuColor 6060/2060 with CXP6000</li> </ul>	DocuColor products with CREO front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.

Product	Response to <a href="#">CERT<sup>®</sup> Advisory CA-2003-12</a>
<b>DocuColor Windows NT based products with EFI front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 12 with X12</li> <li>• DocuColor 12 with EX12</li> <li>• DocuColor 12 with XP12</li> <li>• DocuColor 40 with X40</li> <li>• DocuColor 2045/2060 with EX2000</li> <li>• DocuColor 2045/2060 with EX2000d</li> <li>• DocuColor 2045/2060 with EX2000v</li> <li>• DocuColor 6060 with EXP6000</li> </ul>	DocuColor products with EFI front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.
<b>DocuColor Windows XPe based products with EFI front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 3535 with EX3535</li> </ul>	DocuColor Windows XPe based products with EFI front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.
<b>DocuColor with EFI Splash front-ends:</b> <ul style="list-style-type: none"> <li>• DocuColor 12 with G640</li> <li>• DocuColor 3535 with G3535</li> </ul>	DocuColor products with EFI Splash front-ends do not use Sendmail and are not, therefore, affected by this vulnerability.
<b>Document Centre products (200, 300, 400 and 500 Series)</b>	Document Centre products do not use or contain Sendmail and are not, therefore, affected by this vulnerability.
<b>Document Centre Xerox WIA Driver for Microsoft<sup>®</sup> Windows XP<sup>®</sup></b>	Document Centre Xerox WIA Driver for Microsoft <sup>®</sup> Windows XP <sup>®</sup> does not use Sendmail and is not, therefore, affected by this vulnerability.
<b>DocuPrint N Series products</b>	DocuPrint N Series products do not use Sendmail and are not, therefore, affected by this vulnerability.
<b>DocuSP-based products</b>	DocuSP-based products are affected by this vulnerability. DocuSP patches 3.61.21 and 3.12.29 are available to address this vulnerability. Please contact your Xerox representative for more information
<b>FlowPort</b>	FlowPort does not use Sendmail and is not, therefore, affected by this vulnerability.
<b>iGen3 Creo Spire Color Controller</b>	The iGen3 Creo Spire Color Controller does not use Sendmail and is not, therefore, affected by this vulnerability.
<b>Phaser products</b>	Phaser products do not use Sendmail and are not, therefore, affected by this vulnerability.

Product	Response to <a href="#">CERT® Advisory CA-2003-12</a>
<b>WorkCentre M35</b> <b>WorkCentre M45</b> <b>WorkCentre M55</b>  <b>WorkCentre Pro 35</b> <b>WorkCentre Pro 45</b> <b>WorkCentre Pro 55</b> <b>WorkCentre Pro 65</b> <b>WorkCentre Pro 75</b> <b>WorkCentre Pro 90</b> <b>WorkCentre Pro 32 Color</b> <b>WorkCentre Pro 40 Color</b>	These WorkCentre products do not use or contain 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.