

## Xerox Product Response to CERT<sup>®</sup> Vulnerability Note VU#738331: *Domain Name System (DNS) resolver libraries vulnerable to read buffer overflow*

### 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> Vulnerability Note VU# 738331](#), issued by CERT<sup>®</sup> on October 1<sup>st</sup>, 2002. 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> Vulnerability Note VU# 738331](#) describes a "read buffer overflow" vulnerability in the DNS resolver libraries included with the BIND 4.9.x and 8.2.x branches. The impact is limited to denial of service, and that code execution is not directly possible.

### Xerox Product Response

The table below lists various products and their positions with respect to [CERT<sup>®</sup> Vulnerability Note VU# 738331](#). This document will be updated with additional product information as it becomes available.

Product	Response to <a href="#">CERT<sup>®</sup> Vulnerability Note VU#738331</a>
<b>DigiPath</b>	DigiPath is not impacted by this vulnerability.
<b>DocuColor 1632/2240</b>	DocuColor 1632/2240 products do not use BIND and is not, therefore, affected by this vulnerability.
<b>DocuColor 3535 with EFI Network Controller</b>	The DocuColor 3535 with EFI Network Controller does not use the DNS resolver libraries 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 DNS resolver libraries and are not, therefore, affected by this vulnerability.
<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 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 are not affected by this vulnerability.

Product	Response to <a href="#">CERT<sup>®</sup> Vulnerability Note VU#738331</a>
<b>DocuColor Windows XPe based products with EFI front-ends:</b> <ul style="list-style-type: none"> <li>• <b>DocuColor 3535 with EX3535</b></li> </ul>	DocuColor Windows XPe based products with EFI front-ends are Microsoft Windows based 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 ISC or BSD bind and are not, therefore, affected by this vulnerability.
<b>DocuPrint NPS/IPS Series products</b>	<p>DocuPrint NPS/IPS Series product versions 8.0 and higher include a patch that is automatically installed during software installation.</p> <p>DocuPrint NPS/IPS Series product versions below 8.0 should not normally be configured to use DNS. If custom configuration of the system has enabled name service lookup, the system is potentially exposed to this attack. It is recommended that DNS be changed and the function be performed by static lookups in /etc/hosts.</p>
<b>DocuSP-based products</b>	DocuSP-based products are affected by this vulnerability. Patches are in process and will be announced when available.
<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 ISC or BSD bind 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.