

## Xerox Product Response to US-CERT® Technical Cyber Security Alert TA06-081A: *Sendmail Race Condition Vulnerability*

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 TA06-081A](#), issued by US-CERT® on March 22<sup>nd</sup>, 2006. 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 (NCSA) 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 TA06-081A](#) states that there is a race condition in Sendmail that may allow a remote attacker to execute arbitrary code.

### 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 <a href="#">US-CERT® Technical Cyber Security Alert TA06-081A</a>
<b>Document Centre products (200, 300, 400 and 500 Series)</b>	Document Centre products are not affected by this vulnerability.
<b>DocuPrint NPS/IPS Series products</b>	DocuPrint NPS/IPS Series products do not include Sendmail, therefore, they are not affected by this vulnerability.
<b>DocuSP-based products</b>	DocuSP products are affected by this vulnerability. To avoid this vulnerability the Sendmail service needs to be disabled. This can be done via the DocuSP system-supplied security profiles (low, medium, high), or a user-defined profile can be created that disables the service.
<b>FreeFlow™ Makeready, Process Manager, and Web Services (includes DigiPath)</b>	FreeFlow™ Makeready, Process Manager, and Web Services (including DigiPath) are not affected by this vulnerability.
<b>FreeFlow™ Output Manager FreeFlow™ Print Manager FreeFlow™ SMARTsend™</b>	These FreeFlow products are not affected by this vulnerability.

Product	Response to <a href="#">US-CERT® Technical Cyber Security Alert TA06-081A</a>
<p> <b>WorkCentre 233</b>  <b>WorkCentre 238</b>  <b>WorkCentre 245</b>  <b>WorkCentre 255</b>  <b>WorkCentre 265</b>  <b>WorkCentre 275</b>  <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 233</b>  <b>WorkCentre Pro 238</b>  <b>WorkCentre Pro 245</b>  <b>WorkCentre Pro 255</b>  <b>WorkCentre Pro 265</b>  <b>WorkCentre Pro 275</b>  <b>WorkCentre Pro 32 Color</b>  <b>WorkCentre Pro 40 Color</b>    <b>WorkCentre Pro C2128</b>  <b>WorkCentre Pro C2636</b>  <b>WorkCentre Pro C3545</b> </p>	<p>These WorkCentre products are not affected by this vulnerability.</p>
<p><b>Xerox 1010/2101 Windows NT Copy Server</b></p>	<p>The Xerox 1010/2101 Windows NT Copy Server is not 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.