

Xerox Product Response to CERT® Vulnerability Note VU#681569: *Linux Kernel may fail to properly handle SNMP packets*

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [US-CERT® Vulnerability Note VU# 681569](#), issued by US-CERT® on June 9th, 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® Vulnerability Note VU# 681569](#) states that a memory freeing vulnerability in the Linux kernel module `ip_nat_snmp_basic` can be exploited to create 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® Vulnerability Note VU# 681569
CopyCentre 118 CopyCentre 123 CopyCentre 128 CopyCentre 133 CopyCentre M20	These CopyCentre products are not affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products are not affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products are not affected by this vulnerability.
FaxCentre F12	The FaxCentre F12 is not affected by this vulnerability.
FreeFlow™ Makeready, Process Manager, and Web Services (includes DigiPath)	FreeFlow™ Makeready, Process Manager, and Web Services (including DigiPath) are not affected by this vulnerability.
FreeFlow™ Output Manager FreeFlow™ Print Manager FreeFlow™ SMARTsend™	These FreeFlow products are not affected by this vulnerability.
Phaser products	Phaser products are not affected by this vulnerability.

Product	Response to US-CERT® Vulnerability Note VU# 681569
<p>WorkCentre 118/118i WorkCentre 123 WorkCentre 128 WorkCentre 133 WorkCentre 232 WorkCentre 238 WorkCentre 245 WorkCentre 255 WorkCentre 265 WorkCentre 275 WorkCentre 7655 WorkCentre 7665 WorkCentre C2424 WorkCentre M15 WorkCentre M20/M20i</p> <p>WorkCentre PE16 WorkCentre Pro 123 WorkCentre Pro 128 WorkCentre Pro 133 WorkCentre Pro 423 WorkCentre Pro 428</p>	These WorkCentre products are not 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.