Xerox Security Bulletin XRX10-004
Software update to address Denial of Service vulnerability
v1.0
10/29/10

Background

A vulnerability exists in the firmware for the product listed below. If exploited, this vulnerability could cause a denial of service condition that causes the device to restart. Customer and user passwords are not exposed.

As part of Xerox's on-going efforts to protect customers, a zip file containing the firmware release that addresses this vulnerability is provided for the product listed below. This firmware release can only be installed by a Xerox Customer Support Engineer; please contact the Xerox Support Center to schedule the installation.

The firmware release can be accessed via the links below:
- Xerox 4595 Version 1.224.255 With PostScript® installed, which can be found at
  http://a400.g.akamai.net/7/400/5566/v0001/xerox.download.akamai.com/5566/zip/fuhjin-XC-ps-dld-1.224.255.zip
- Xerox 4595 Version 1.224.255 Without PostScript® installed, which can be found at
  http://a400.g.akamai.net/7/400/5566/v0001/xerox.download.akamai.com/5566/zip/fuhjin-XC-dc-dld-1.224.255.zip

The solution for this vulnerability is classified as **Important**.

Acknowledgment

Xerox wishes to thank chap0 of the corelan team for initially notifying us of this vulnerability.

This software solution applies to network-connected versions[1] of the following product:

Xerox	
4595	

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.

---

[1] If the product is not connected to the network, it is not vulnerable and therefore no action is required.