# XEROX SECURITY BULLETIN XRX06-006 (This bulletin v1.1 supersedes XRX06-003.)

Cumulative update to address multiple security vulnerabilities.

System Software Versions 12.060.17.000, 14.060.17.000 or 13.060.17.000, depending on whether the product is a WorkCentre® or WorkCentre® Pro, is an update to System Software Versions 12.050.03.000, 14.050.03.000 and 13.050.03.000, respectively, that includes security fixes for the system software. See Appendix A to obtain the *.060.17.000 System Software[1].

Customers are strongly encouraged to upgrade their devices to System Software Version 12.060.17.000, 14.060.17.000 or 13.060.17.000, respectively. Please follow the procedures in Appendix A to obtain the updated system software. Utilize the customer install instructions that come with the system software for updating your device. The table below shows the corresponding Network Controller version for each of these three System Software Versions.

| Products | System SW Version | Network Controller Version |
|---|---|---|
| WorkCentre 232/238/245/255/265/275 | 12.060.17.000. | 040.022.00115 |
| WorkCentre Pro 232/238/245/255/265/275 | 13.060.17.000. | 040.022.50115 |
| WorkCentre 232/238/245/255/265/275 with PostScript option | 14.060.17.000. | 040.022.10115 |

This software is now Common Criteria validated and is listed on the National Information Assurance Partnership's Validated Products List at http://www.niap-ccevs.org/cc-scheme/vpl/.

## Background

System Software Versions 12.060.17.000, 14.060.17.000 and 13.060.17.000 are maintenance releases incorporating security fixes to System Software Versions 12.050.03.000, 14.050.03.000 and 13.050.03.000, respectively. The update incorporates security fixes for the following vulnerabilities in the ESS/ Network Controller and MicroServer Web Server code:

- TCP/IP hostname on the Web User Interface vulnerable to command injection.
- Scan-to-mailbox folder name field on the Web User Interface vulnerable to command injection.
- Microsoft Networking configuration parameters on the Web User Interface vulnerable to command injection.
- Browser permissions could allow unauthorized access.
- TFTP/BOOTP auto configuration option could permit unauthorized configuration of settings.
- Web services requests can be made using HTTP instead of HTTPS.
- Signature of e-mail messages can be hijacked to display improper items.
- Scan-to-mailbox feature could allow anonymous, unauthenticated download of secure files.
- Device did not keep accurate time, so time stamps in audit logs were incorrect.

If these vulnerabilities were successfully exploited, security functions might not work properly and an attacker could gain unauthorized access and make unauthorized changes to the system configuration. Customer and user passwords are not exposed.

In addition to the above fixes, we have enhanced the security of the DLM upgrade files by incorporating digital signatures.

[1] * will be either a 12, 13, or 14 depending on whether the product is a WorkCentre® or a WorkCentre® Pro

**Products Affected:**

| WorkCentre® | WorkCentre® Pro |
|---|---|
| 232 | 232 |
| 238 | 238 |
| 245 | 245 |
| 255 | 255 |
| 265 | 265 |
| 275 | 275 |

## Appendix A

### Obtaining the latest System Software Version

To obtain the latest general release:

a) Use a browser to navigate to www.xerox.com.
b) Select the link called "Support & Drivers".
c) Select "Multifunction".
d) Select "WorkCentre" or "WorkCentre Pro" depending on your model.
e) Locate the link for your WorkCentre model.
f) Select "Drivers & Downloads".
g) Select the link for "Firmware & Machine Upgrades".
h) Select the link for "System software version xx.xx.xx.xxx install instructions" and print or save these instructions.
i) Select the link for "System Software Upgrade Version xx.xx.xx.xxx" and save the file to your computer.
j) Once downloaded, extract the files to your desktop.
k) Review the "System Software Install Instructions" that you saved for important information about upgrading your device.
l) Upgrade the device.
m) Return to the "Install the Patch" section of the document referenced above.

## Disclaimer

The information 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.