XEROX SECURITY BULLETIN XRX06-004

Cumulative update to address multiple security vulnerabilities.

System Software Versions 12.050.03.000, 14.050.03.000 or 13.050.03.000, depending on whether the product is a WorkCentre® or WorkCentre® Pro, is an update to System Software Versions 12.027.24.000, 14.027.24.000 and 13.027.24.000, respectively, that includes security fixes for the system software. See Appendix A of the Patch Install Instructions to obtain the *.50.03.000 System Software[1].

Customers are strongly encouraged to upgrade their devices to System Software Version 12.050.03.000, 14.050.03.000 or 13.050.03.000, respectively. The table below shows the corresponding Network Controller version for each of these three System Software Versions.

System SW Version	Network Controller Version
12.050.03.000.	040.010.01172
13.050.03.000.	040.010.51172
14.050.03.000.	040.010.11172

Background

System Software Versions 12.050.03.000, 14.050.03.000 and 13.050.03.000 are maintenance releases incorporating security fixes to System Software Versions 12.027.24.000, 14.027.24.000 and 13.027.24.000, respectively. The update incorporates security fixes for the following vulnerabilities in the ESS/ Network Controller and MicroServer Web Server code:

- Web User Interface authentication can be bypassed.
- US-CERT Technical Cyber Security Alert TA04-174A.
- Samba version must be upgraded to address multiple vulnerabilities.
- SNMP Agent does not return error for non-writable objects.
- SNMP Authentication failure traps cannot be enabled nor generated.
- Network controller Vulnerability: http TRACE XSS attack.
- Attached PS script causes ops3-dmn to crash with core dump; DoS attack.
- SMB "Homes" share visible.
- SMB file system browsing possible.
- Audit Log- anonymous download possible.
- HTTP Security issues.
- Bypass security and boot Alchemy using USB thumb drive (or other method).
- Scan "Validate Repository SSL Certificate" not checking FQDN.
- Certain file permissions should be tightened.
- Linux Security - Need to fix kernel vulnerability CAN-2003-0643 - socket issue.
- Port 443 is always active- httpd.conf misconfiguration.
- Postgress port block.
- SNMP Authentication failure traps cannot be enabled nor generated.
- CRITICAL fragments of remnant user data in http.log after Immediate Image Overwrite (IIO).
- IIO Error Message on LUI if overwrite fails.
- When Held Job is deleted, IIO reports failure.
- On Demand Image Overwrite failures for overwrites larger than 2GB.

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

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.

Products Affected:

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

Appendix A

Obtaining System Software Version *.50.03.000

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 *.50.03.000 install instructions” and print or save these instructions.
i) Select the link for “System Software Upgrade Version *.50.03.000” 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.
l) Upgrade the device.
m) Return to the “Install the Patch” section.

Disclaimer