XEROX®

Technology | Document Management | Consulting Services

Xerox Multifunction Systems and Network Security: What You Should Know

Xerox is committed to helping customers maintain a secure network environment, particularly as it relates to the use of multifunction products, which print, copy, fax and scan. Since all Multifunction Products (MFPs) -- regardless of vendor -- contain hard drives and software, MFPs require the security precautions associated with other network peripherals.

Before bringing a product to market, we extensively test for security vulnerabilities in our software. However, there is inherent risk with any network peripheral or device that contains software. It is always possible that new ways to break the software will be discovered. We take security vulnerabilities seriously and move immediately to provide a solution.

Xerox provides more security for potential entry points to its MFPs than any of our competitors and continues to update those security functions on a regular basis. We also offer the broadest range of multifunction systems that meet the internationally recognized standard for security and have earned NIAP Common Criteria full system certification.

At a recent Black Hat IT security conference in Las Vegas, Brendan O'Connor, an independent security researcher, presented a session on vulnerability in Xerox WorkCentre and WorkCentre Pro 200 series multifunction systems. We learned of this security vulnerability in January of this year. We appreciate Mr. O'Connor bringing this to our attention. Concurrently, we were working on a fix and in February posted a patch for upgrades on our website. Since establishing the www.xerox.com/security site in 2004, we have routinely posted system updates and patch information for customers to access.

The upgrade was included in the manufacturing process and provided to Xerox service representatives, who routinely install system software upgrades on machines in the field.

XEROX®

Technology | Document Management | Consulting Services

Only a narrow selection of monochrome products was open to this vulnerability. The only models affected are listed in the table below:

Model	**System Software**	**BIOS**
WorkCentre **Pro** 232/238, 245/255, 265/275	**13**.27.24.000 through **13**.27.24.012	v7.02 or 7.04
WorkCentre w/PS Option 232/238, 245/255, 265/275	**14**.27.24.000 through **14**.27.24.012	v7.02 or 7.04
WorkCentre 232/238, 245/255, 265/275 (Europe only)	**12**.27.24.000 through **12**.27.24.012	v7.02 or 7.04

No other Xerox products are affected.

Media reports indicated our machines might still be at risk, despite the upgrade. We have thoroughly retested the upgrade and are confident the upgrade provides full security against the vulnerabilities which were reported. Once we were made aware of the issue, we put a fix in place, submitted and passed NIAP Common Criteria full system certification with the fix, updated our security web site for customer communication, and put in place a process to ensure all of our customers who may require this upgrade are effectively supported.

As a customer, here is what you can do:

Customers may contact their Xerox representative to schedule a system upgrade. Please have your serial number ready when you call.

Customer Support Phone Numbers

United States	800-821-2797
Austria	+43 1 2079000
Belgium	+32 02 713 14 53
Belgium	+32 02 713 14 52
Canada	800-939-3769
Denmark	+45 70107288
Finland	+358 09 693 79 666
France	0825 012 013
Germany	+49 180 5004392
Greece	210 6646358
Ireland	+353 1890 92 50 50
Italy	+39 199 11 20 88
Luxembourg	480123
Netherlands	+31 020-6563620
Norway	+47 81 500 308

XEROX®

Technology | Document Management | Consulting Services

Portugal, Hardware	+351 210 400 500
Portugal, Software	+351 210400590
Spain	+34 902 160 236
Sweden	+ 46 0771 178 808
Switzerland	+41 43 299 9001
Switzerland	+41 43 299 9000
Switzerland	+41 43 299 9002
UK	+44 0870 9005501

An upgrade is also available at the Support & Drivers page of www.xerox.com. For the full details about checking the versions of software on your device and the procedures to upgrade the device, please see the instructions document at the Support & Drivers page of www.xerox.com.

- Select “Multifunction” as your product type
- Select the product family “WorkCentre” or “WorkCentre Pro” for your particular model.
- Select “Drivers & Downloads” link for your particular model.
- When the webpage is refreshed, select the “Firmware & Machine Upgrades" link. Installation instructions and the current version of system software for your product are now available for download.

Most vulnerabilities will be eliminated with the completion of this upgrade. However, this upgrade, System Software *.50.03.000, completes the security update only if your system has BIOS version 7.07 or higher. The asterisk represents version 12, 13 or 14, depending upon your system’s configuration.

Frequently Asked Questions

Q: What is the security issue that has been reported?
A: Since all MFPs -- regardless of vendor -- contain hard drives and software, they require security precautions associated with other network peripherals. Earlier this year, as part of our ongoing security efforts, Xerox became aware of a potential vulnerability in the start up mode of WorkCentre 200 multifunction products. While we were validating the vulnerability, Brendan O’Connor, an independent security researcher let us know that he had discovered a similar issue. In February, we issued an upgrade to address the problem. We are not aware of any customer problems having been reported to date to Xerox security experts. Customers with specific questions or concerns should contact their Xerox representative or go to the Xerox security website. Please refer to table above for a complete list of phone numbers.

XEROX®

Technology | Document Management | Consulting Services

Q: What is being done to protect customers?
A: Xerox is committed to helping customers maintain a secure network environment. As soon as this issue was discovered, experts within Xerox began developing a solution to correct the concern. As part of our normal processes, the solution was included in the manufacturing process and provided to Xerox service representatives. Depending on machine configuration, customers may download the updated software from www.Xerox.com or call a customer support representative for further assistance. Ensure you have your machine serial number ready when you call. The customer support numbers are listed in a separate table in this document.

Q: Is there is a way around this upgrade? What is Xerox doing to address that concern?

A: As part of the Black Hat presentation, Mr. O'Connor discussed the possibility of an additional vulnerability. He shared with us the method he used to try and gain additional access. We have extensively tested this and remain confident that the current upgrade fully addresses the problem and that no additional patch is necessary. Xerox is committed to providing its customers with a secure environment. As always, if any new problem is discovered and if a patch is required we will post information immediately to www.xerox.com/security

Q: What machines were affected?
A: Only the models listed in the table below are affected:

Model	System Software	BIOS
WorkCentre **Pro** 232/238, 245/255, 265/275	**13**.27.24.000 through **13**.27.24.012	v7.02 or 7.04
WorkCentre w/PS Option 232/238, 245/255, 265/275	**14**.27.24.000 through **14**.27.24.012	v7.02 or 7.04
WorkCentre 232/238, 245/255, 265/275 (Europe only)	**12**.27.24.000 through **12**.27.24.012	v7.02 or 7.04

Note: The CopyCentre versions of the 200 series are not affected. Only systems and configurations listed above require upgrading.

XEROX®

Technology | Document Management | Consulting Services

Q: How do I know if my machine has the upgrade?
A: The chart below indicates the models and software versions that contain the upgrade:

Model	System Software	BIOS
WorkCentre **Pro** 232/238, 245/255, 265/275	**13**.27.24.015 or higher	v7.07
WorkCentre w/PS Option 232/238, 245/255, 265/275	**14**.27.24.015 or higher	v7.07
WorkCentre 232/238, 245/255, 265/275 (Europe only)	**12**.27.24.015 or higher	v7.07

Customers may check the system software levels by accessing the device webpage via WorkCentre Internet Services, print a configuration report at the device, or contact a Xerox customer support representative for assistance. Have your serial number ready when you call. Please refer to customer support table for appropriate phone numbers.

Preferred method: Access WorkCentre Internet Services, by entering the IP address for the required device in a browser URL. When Internet Services are displayed, select the Properties tab, select General Setup and select Configuration. Scroll to the Printer Setup section. Compare the System Software and BIOS version to the version listed above. System Software version *.27.24.015 or higher with BIOS version 7.07 or higher contain all the required patches.
***Depending on model, the version may start with 12, 13, or 14.**

To print a configuration report, select Machine Status at the device user panel. Select the Print Reports button, then select the Print System Configuration Report. This report will also provide the IP address for the above procedure if the IP address is not known.

Q: How are you informing customers about security patches?
A: As with all security bulletins or patches, we post the information on our website, www.xerox.com/security. In this case, our service reps have the upgrade as part of a routine maintenance pack that gets installed on customer equipment. To help educate customers about security issues involved in networked systems, Xerox is hosting Security Summits across North America. We've already held summits in Boston and Washington, DC. Later this year, we'll bring the summits to Stamford, CT, Toronto, Seattle, Chicago and Cincinnati. Xerox also recently launched an IT Xchange Webcast on security to extend the Security Summit information to an even broader audience. To access the Webcast "The Document Security Imperative: Beyond PCs and Firewalls," visit www.xerox.com/security.

XEROX®

Technology | Document Management | Consulting Services

Q. Are there any cases that you aware of where unauthorized individuals have used a multifunction, networked device to illegally enter an enterprise network?
A: No, we don't know of any such cases.

Customers with questions or concerns about security and their Xerox equipment can visit www.xerox.com/security or call your Xerox Customer Service Representative. Please see table below for customer support numbers:

Customer Support Phone Numbers

United States	800-821-2797
Austria	+43 1 2079000
Belgium	+32 02 713 14 53
Belgium	+32 02 713 14 52
Canada	800-939-3769
Denmark	+45 70107288
Finland	+358 09 693 79 666
France	0825 012 013
Germany	+49 180 5004392
Greece	210 6646358
Ireland	+353 1890 92 50 50
Italy	+39 199 11 20 88
Luxembourg	480123
Netherlands	+31 020-6563620
Norway	+47 81 500 308
Portugal, Hardware	+351 210 400 500
Portugal, Software	+351 210400590
Spain	+34 902 160 236
Sweden	+ 46 0771 178 808
Switzerland	+41 43 299 9001
Switzerland	+41 43 299 9000
Switzerland	+41 43 299 9002
UK	+44 0870 9005501