Konica Minolta bizhub CS Remote Care* 2.10

Security Testing

11 December 2018

DR180718I

Miercom.com

www.miercom.com

Contents

*CS Remote Care is also known as vCare in the US and Canada, and three other names elsewhere in the world.

1.0 Executive Summary

Multifunction Products (MFP) are devices that allow businesses to extend their knowledge, marketing and daily operations through printing, copying, scanning, faxing and more. What makes MFP services exceptional is providing optimal customer care. MFP management assists businesses with diverse services – some seemingly minute tasks, such as toner replacement, and others for support of large internal network issues that cause disruptive and costly downtime.

To keep businesses running smoothly and continue driving productivity, operations are automated with cloud-based monitoring and device reporting. MFP components are no different than any other network endpoint and are equally susceptible to threats. Miercom recommends MFP management solutions are encouraged to be as secure as possible when handling these devices.

Konica Minolta Business Solutions USA, Inc. engaged Miercom to perform a comprehensive security assessment of the latest version of *bizhub CS Remote Care* (version 2.10R1) and 7 *bizhub* products representative of their entire MFP range that served as endpoints in the test environment. By participating in Miercom's Certified Secure program, these products were subjected to vulnerability testing in a real-world environment to analyze protective functionality and identify opportunities for security hardening.

Key Finding

No prominent vulnerabilities were found in the email server, database server, Windows DCA component, Raspberry Pi DCA, web application, communication server, WebDAV server or engines.

Based on our findings, we award the Konica Minolta *bizhub CS Remote Care* Solution the ***Miercom Certified Secure*** accreditation for its impressive, hardened solution which protects against vulnerabilities and exploits in an enterprise environment.

Robert Smithers

CEO

Miercom

2.0 Test Summary

Table 1: Component Security Status

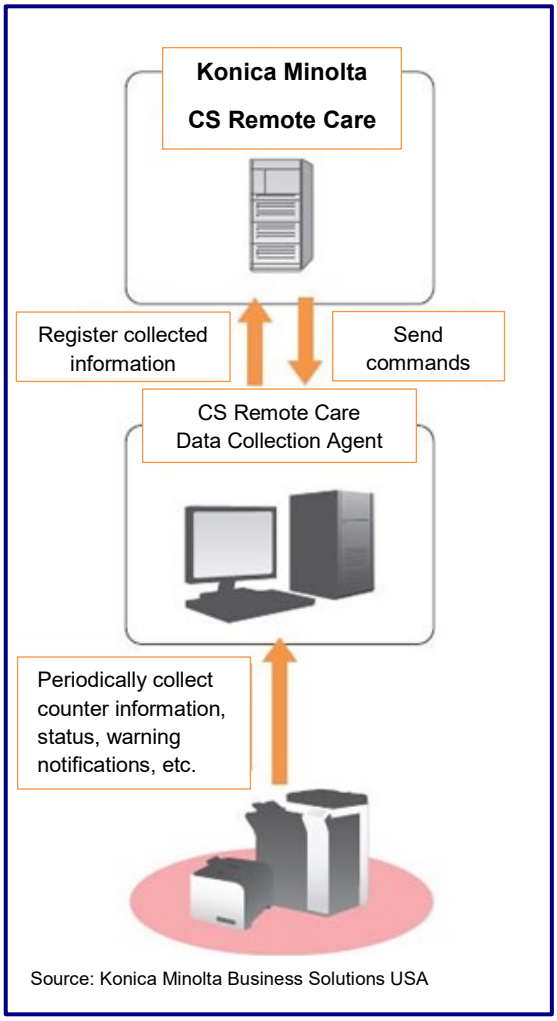
Component Tested	Pass/Fail
Email Server	**Pass**
Database Server	**Pass**
Windows DCA	**Pass**
Raspberry Pi DCA	**Pass**
Konica Minolta Web Application	**Pass**
Communication Server	**Pass**
WebDAV Server	**Pass**
Engine	**Pass**

3.0 Product Overview

Konica Minolta *bizhub CS Remote Care** is a software system that enhances customer care and management of Multifunction Products (MFP) with automated, secure services which enhance business productivity. This solution helps businesses with the following:

- Print, copy, scan and fax time-sensitive materials to drive efficiency and growth
- Offer immediate and thorough consulting during critical application use
- Automated, remote and secure services to reduce downtime and IT staff costs
- Easy-to-use interfaces
- "Invisible" diagnosis and maintenance of internal issues using cloud services
- Responsive support team for personal attention to business core values and expectations

bizhub CS Remote Care is the name used in the Europe and Japan for the device management and communications system introduced in 2008 by Konica Minolta Business Solutions USA, Inc. The system is known as *vCare* in the United States and Canada, and three other names elsewhere in the world.



Source: Konica Minolta Business Solutions USA

bizhub and bizhub PRO products manufactured since 2005 can be managed remotely by the system. At present, October 2018, it is managing close to 400,000 products in the United States and Canada and over a 1,000,000 worldwide.

bizhub CS Remote Care consists of embedded technology within the Konica Minolta product and a Cluster of Servers running the CS Remote Care Solution. New in *bizhub CS Remote Care 2.10* is the CS Remote Care Data Collection Agent, also deployed worldwide as the CS Remote Care Data Collection Application, which runs on a computer on the end-user organization's enterprise network and can manage up to 10,000 bizhub, bizhub PRO and 3rd Party products. This node regularly collects information about operational status and sends it to a Konica Minolta branch office or authorized reseller that provides the management service.

The information enables the service provider to initiate appropriate action to keep the products in optimal operating condition.

bizhub and bizhub PRO devices manufactured since 2011 communicate with bizhub CS Remote Care via one-way e-mail or HTTP(S) one-way or bidirectional communication based on the reporting schedule set within the device. The CS Remote Care Data Collection Agent utilizes network polling to transmit data to the system via HTTPS for bizhub A4 Printers and third-party devices.

Table 2: Products and Applications Tested

Products Tested	
bizhub C458	
bizhub C308	
bizhub 4752	
HP LaserJet M553	
KIP 940	
Lexmark T650	
Xerox Phaser	
Application	**Version**
bizhub CS Remote Care[1]	V2.10R1
DCA (Windows)	1.8R1
DCA (Raspberry Pi)	2.3R1

[1] The bizhub CS Remote Care Web Application, KMCore and Server are all at version v.2.10R1

4.0 How We Did It

In a lab environment, Miercom evaluated the Konica Minolta *bizhub* CS Remote Care system by subjecting its individual components to vulnerability testing and analysis. Miercom used NMAP, Nessus and McAfee Vulnerability Manager (MVM) to carefully inspect components for security flaws. To obtain the Miercom Certified Secure accreditation, Miercom requires that no high-level vulnerabilities be found.

The test environment consisted of an email server, database server, two DCA servers, a Web Distributed, Authoring and Versioning (WebDAV) server, communications server, ten MFPs, and four third-party devices.

4.1 Test Tools

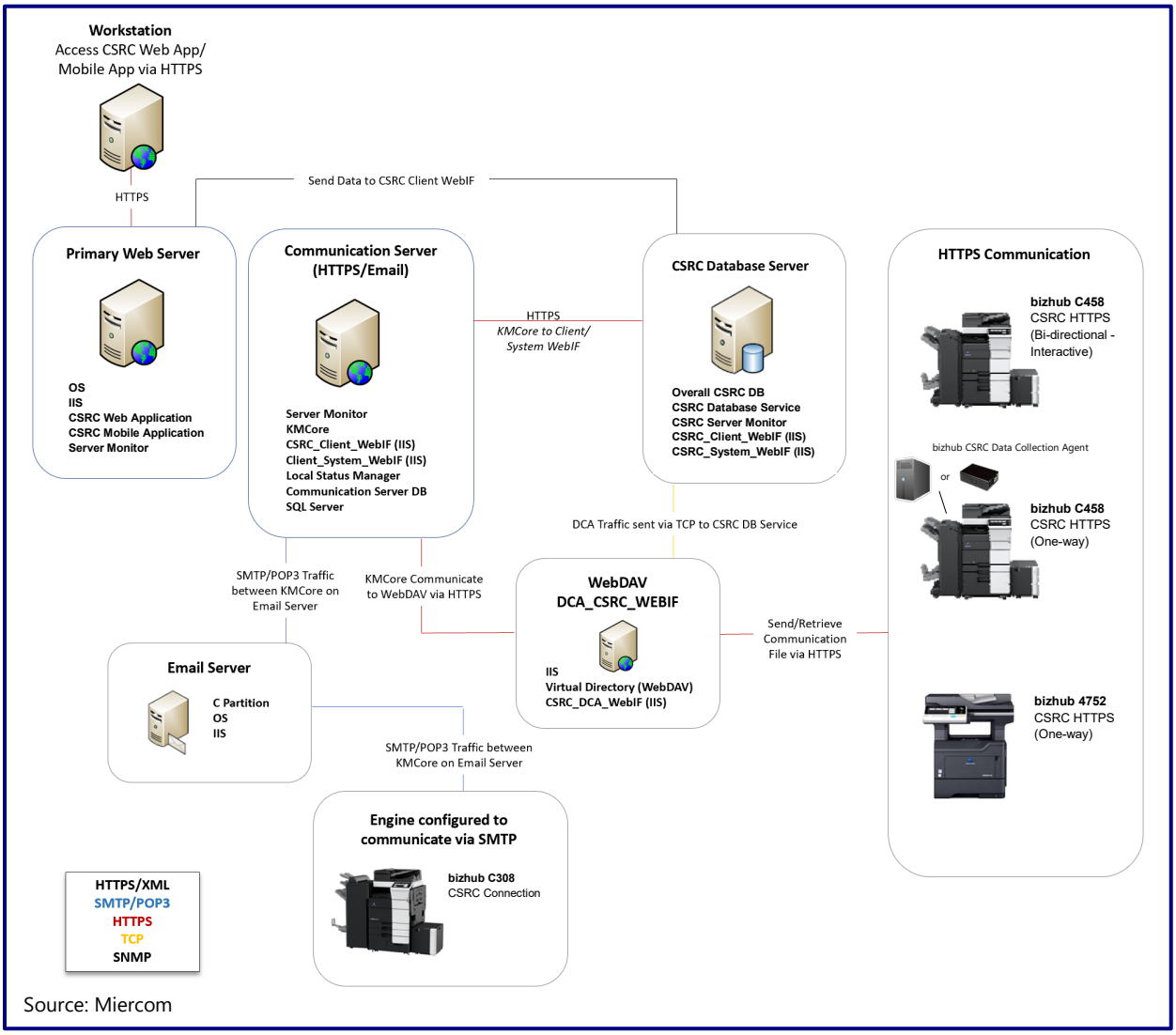
Source: Miercom

Nmap 7.12 scanner is a standard tool to help identify open ports and version information, where applicable, as the first insight into product communication. It offers custom probing to solicit responses to identify active IP addresses (used by host/network device) and scans active addresses for vulnerabilities that would affect the network using its database of about 2,200 known services to corresponding ports (e.g. SMTP for mail server, HTTP for webserver). When a response does not match an entry in its database, Nmap uses 6,500 pattern matches for more than 650 protocols to identify the vulnerability source.

Nessus vulnerability scanner locates exploitable areas to help penetration testers and other security consultants to immediately remediate potential attack points of entry. This scan consists of 55,000 plugins from the 108,191 published by Tenable. Each plugin attempts to identify vulnerabilities to highlight security shortcomings of the product.

McAfee Vulnerability Manager performs similarly to Nessus, with some deviations in content. The MVM engine has the capability to scan for over 4,700 vulnerabilities, along with identifying common security issues such as weak passwords.

4.2 Test Bed Diagram



Source: Miercom

The network diagram above outlines the lab environment configuration, consisting of many more components than seen in a typical CS Remote Care deployment. This expansive setup accounts for multiple deployment scenarios available with the CS Remote Care product. This test bed covers deployments which utilize direct HTTPS communications with the CS Remote Care (CSRC) DCA, SNMP to a local DCA, which then directs information to the CSRC DCA via HTTPS and SMTP/POP3 communications to a local email server to a communication server. The CSRC WebDAV and communication server communicate with the CS Remote Care database server, which logs vital system information. Together, these components provide customers with a seamless printer experience.

5.0 Results

5.1 Email Server

IBM NOTES 9
Windows Server 2008 R2

Status: PASS

5.2 Database Server

Windows Server 2012 R2

Status: PASS

5.3 Windows DCA

Windows Server 2012 R2

Status: PASS

5.4 Raspberry Pi DCA

Status: PASS

5.5 Konica Minolta Web Application

Windows Server 2008 R2

Status: PASS

5.6 Communications Server

Windows Server 2008 R2 SP1

Status: PASS

5.7 WebDAV Server

Windows Server 2008 R2

Status: PASS

5.8 Engine

Status: PASS

6.0 Conclusion

Security Assessment Summary

All findings presented in this report show the Konica Minolta *bizhub* CS Remote Care products provide flawless mitigation through all tested vulnerability scenarios. Thorough testing of different *bizhub* CS Remote Care system components revealed superior protection against network threats that are common to real-world deployments. Based on these impressive results, Konica Minolta receives the ***Miercom Certified Secure*** accreditation for its *bizhub* CS Remote Care products, *bizhub PRO* products, applications and third-party devices.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.