# Security Testing Summary of
# Konica Minolta bizhub vCare 2.10
# Device Management and Communications System
# and Various bizhub Products


**SR180630**

**July 2018**

**Miercom**

www.miercom.com

## Overview

Konica Minolta Business Solutions USA, Inc. engaged Miercom to perform a comprehensive security assessment of the latest version of *bizhub vCare, 2.10*, and six bizhub products that served as endpoints of the test environment.

Individual components of *bizhub vCare 2.10* subjected to vulnerability scans and protocol mutations attacks included vCare server, vCare database server, vCare Web interface and the vCare Data Collection Agent.

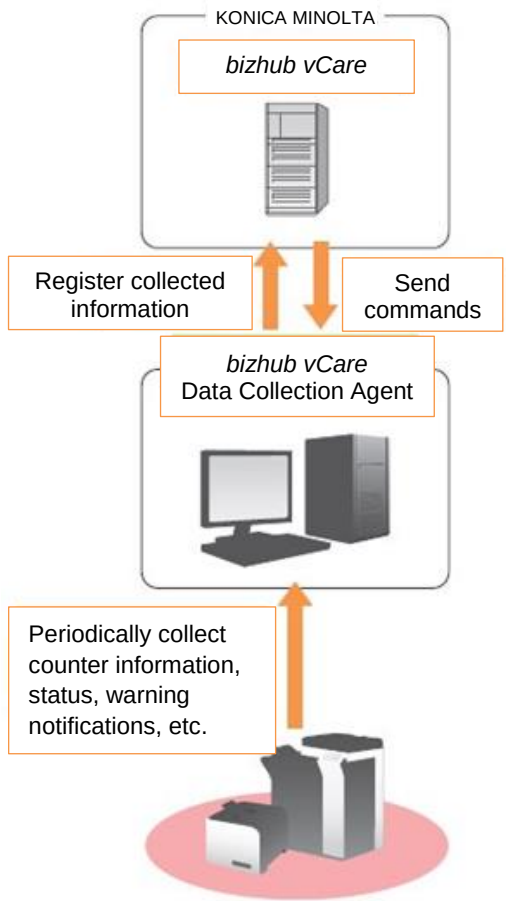
The purpose of testing was to attempt to disrupt communications between bizhub vCare and the endpoints.

## About *bizhub vCare 2.10* and bizhub Products

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

bizhub vCare™

Remote service that's always there for you




Device manufactured by KONICA MINOLTA

Source: Konica Minolta Business Solutions USA

bizhub and bizhub PRO products manufactured since 2005 can be managed remotely by the system. At present, July 2018, it is managing more than 200,000 products in the United States and Canada and approximately 800,000 worldwide.

*bizhub vCare* consists of embedded technology within the Konica Minolta product and an off-site vCare server. New in *bizhub vCare 2.10* is the vCare 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 1,000 bizhub or bizhub PRO 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.

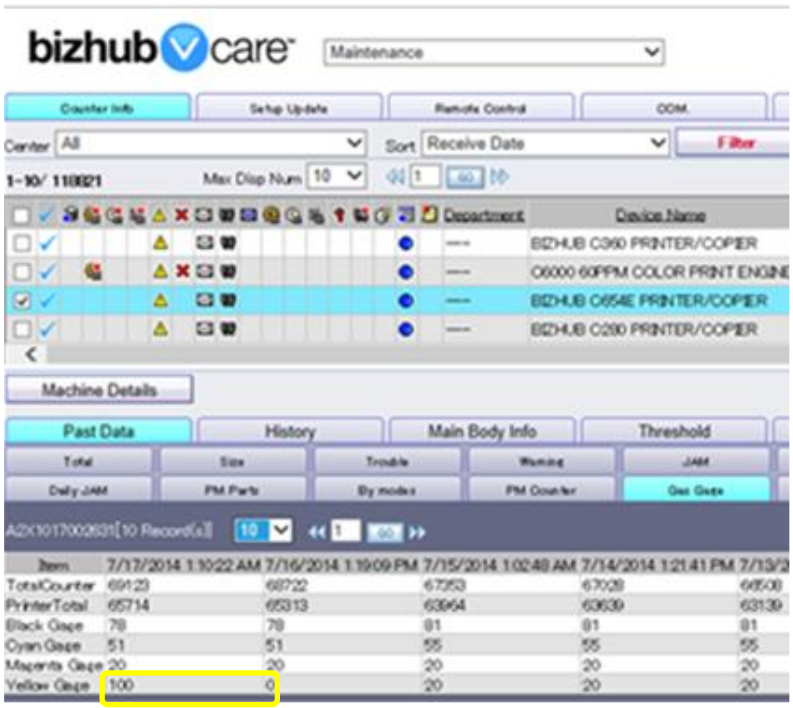
bizhub and bizhub PRO devices manufactured since 2011 communicate with *bizhub vCare* via one-way e-mail or one-way HTTP(S) based on the reporting schedule set within the device. The vCare Data Collection Agent utilizes network polling to transmit data to the system via HTTPS.

Older devices communicate with *bizhub vCare* by way of short, bidirectional e-mail messages. The service provider assigns and manages email addresses and HTTP(S) credentials for all bizhub and bizhub PRO products on the enterprise network of customers.

bizhub or bizhub PRO products send service alerts, warnings and jam notifications in real-time as well as daily messages to *bizhub vCare* to ensure that the service provider can act proactively if needed.

That data includes:

- Current meter reading, which has enabled the service organization to automate billing
- Level of consumables, such as toner in the graphic to the right, which can automatically generate an immediate delivery if required
- Error code alerts, which pinpoint operational problem(s) and, if necessary, can prompt a service technician to be dispatched immediately with the proper repair or replacement part(s)



Source: Konica Minolta Business Solutions USA

- Status of key components, which notifies the service provider when a part critical to optimal print quality, such as a fuser or laser, is nearing the end of its service life

The bizhub products in the test environment were: **20P** and **25e** "all-in-one" desktop devices, **4700P** high-resolution monochrome laser printer, **C360** and **C754e** standalone multifunction printers, and **PRESS C1100** digital press for production printing.

## Key Findings and Conclusions

- **bizhub vCare does not pose a security risk for enterprise network of end-user organizations**
- **bizhub vCare Web interface as well as database and Data Collection Agent (DCA) servers exhibited resilience against vulnerability scans by Nessus and Nmap**
- **Components of bizhub vCare in the local test environment and the data center that hosts the system for North America were impervious to a variety of protocol mutation attacks**

## Security Functionality of *bizhub vCare*

The system uses an external e-mail server. Also, the e-mail payload is encrypted. The data is statistical and non-sensitive. With an effective firewall located at the customer premises, open ports are unlikely to allow undesired access.

## Test Conditions

The bizhub products in the local test environment had no security countermeasures, a "worst-case" scenario for testing security vulnerabilities.

The vCare Data Collection Agent application also was in the test environment, on a Windows 7 laptop that was not hardened. This, of course, would not occur in a real-world deployment.

The test environment was connected via a Netgear hub to the production *bizhub vCare* system in the Konica Minolta Business Solutions USA data center in Ramsey, NJ. Components of *bizhub vCare* tested that reside in the data center were a vCare server and a vCare database server.

## Test Tools Used in Vulnerability Scans and Protocol Mutation Attacks


Nessus from Tenable Network Security


Nmap from nmap.org


Spirent Studio Security software and Mu-8000 appliance


OmniPeek from WildPackets


Wireshark

Two vulnerability scanners, **Nessus** from Tenable Network Security and **Nmap** from nmap.org, were utilized to attempt to identify vulnerabilities in *bizhub vCare* and the bizhub products.

A Spirent solution, **Studio Security software** housed on a **Mu-8000 appliance**, directed protocol mutation attacks against one or more of the following: bizhub products, vCare Web interface, vCare server, vCare database server and vCare Data Collection Agent server. The attacks included many known (published) vulnerabilities. Also, external attacks using test cases and customer scripts were utilized.

The **OmniPeek** network analyzer from WildPackets and the **Wireshark** packet analyzer were used to monitor and capture Simple Network Management Protocol (SNMP) traffic between bizhub devices and the vCare Data Collection Agent server. Recovery alert conversations between the bizhub products and the vCare server were captured.

## Results

Nessus was utilized to perform preliminary port scans on the vCare Web interface, vCare database server and the vCare Data Collection Agent server.

Of the more than 60,000 plugins for both local and remote vulnerability checks, approximately 12,000 were chosen that we deemed appropriate for the test environment. Those plugins were in the categories that included:

- Backdoors (Operating System Level testing)
- Common Gateway Interface Abuses (specific to Web management)
- Common Gateway Interface Abuses: Cross-Site Scripting (specific to Web management)
- Firewalls (Operating System Level checks)
- Remote Shell Access (Operating System Level backdoors)
- Service Detection (identification of unknown services)
- SNMP (management protocols and configuration)
- Web Services (specific to Web management)
- Microsoft Windows (agent installation)

The performance by *bizhub vCare* and the bizhub products was near-flawless. Out of all of the tests performed, only 33 required further analysis.

### Highlights of Nessus Vulnerability Scans

| Attack | Result |
|---|---|
| PCI Data Security Standard Compliance | **Pass** |
| Simple Network Management Protocol | **Pass** |
| Service Detection | **Pass** |
| HTTP | **Pass** |
| HeartBleed SSL | **Pass** |

Source: Miercom, July 2018

The Nmap vulnerability scan did not reveal any open ports. It did reveal that the vCare Web interface, the vCare database server and the vCare Data Collection Agent had ports 21, 139, 443 filtered. However, the ports were responsive.

Therefore, our conclusion is that the vCare Web interface, the vCare database server and the vCare Data Collection Agent are secure. Ports 21, 139 and 443 were filtered appropriately, in a way that allows only authenticated users to communicate.

Lastly, *bizhub vCare* and the bizhub products were impervious to all four protocol mutation attacks. The type of attack and the bizhub components challenged follow:

- Transmission Control Protocol: bizhub products as well as bizhub vCare and (DCA) servers
- Dynamic Host Configuration Protocol: bizhub products and vCare server
- HTTP/HTTPS: bizhub vCare and bizhub Data Collection Agent servers
- Address Resolution Protocol: bizhub vCare database server and bizhub Web interface

## Conclusion

Miercom conducted a battery of assaults to attempt to disrupt the communication between the bizhub products tested and *bizhub vCare*. It was not possible to hack into *bizhub vCare* through the network ports. As a result, the ability of the bizhub products to function, be managed or actively provide information to *bizhub vCare* was not affected.

The uptime management benefits of utilizing *bizhub vCare* are tremendous. The system maximizes uptime of bizhub and bizhub PRO products through real-time service alerts. We observed bizhub products provide real-time alerts in the form of one-way e-mail for critical events, such as a cooling fan failure, consumables needed and service required.

We see no risk and only benefits to implementing *bizhub vCare* on the enterprise network of Konica Minolta customers. The requirements to use the system should not concern even the most security conscious customers. We do recommend that any organization employ layered, active security on its enterprise network.

The Konica Minolta *bizhub vCare 2.10* device management and communications system and the bizhub 20P, 25e, 4700P, C360, C754e and PRESS C1100 have earned Miercom **Certified Secure**.


## About Miercom

Founded in 1988, Miercom pioneered the business of independent, hands-on testing of products and services for the enterprise network and communications industry. For 30 years the company has provided test services and consulting and is considered a leading independent test facility.

Private test services include competitive product analyses as well as individual product evaluations. Miercom features comprehensive certification and test programs including: **Performance Verified**, **Certified Secure**, **Certified Green** and **Certified Reliable**. These certifications are recognized by networking vendors and end-user organizations as an accurate, unbiased validation of the ability of the product or service to perform in a real-world network.

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. For more information about Miercom testing and certifications as well as consulting services, please visit www.miercom.com.