Security White Paper

Konica Minolta bizhub vCare with Secure HTTP/HTTPs Device Relationship Management System

August 2010

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Multifunctional printers (MFPs) from Konica Minolta Business Solutions U.S.A., Inc. (Konica Minolta) with uptime management provided by vCare Device Relationship Management System proved in thorough lab testing and onsite assessment to provide superior resiliency and resistance to network compromise and achieved Miercom Certified Secure for the third consecutive year.

Miercom tested the overall security of Konica Minolta's device relationship management system bizhub vCare (vCare), complete with bizhub C652DS series, C360 series, bizhub 423 series, bizhub 500 and 350 series. Also included are the bizhub PRO 1050, bizhub PRO 1200, bizhub PRO C6501, and bizhub PRESS C8000 digital presses, as part of an ongoing security assessment of the product solution under the Miercom Certified Secure Program. The vCare component was tested as a complete solution while Miercom engineers assessed the dialog between the vCare Service Center and the MFPs for potential vulnerability. We evaluated the overall capability of vCare to provide uptime management of networked MFPs. We reviewed the security of the MFPs themselves for vulnerability to DOS and other attacks with specific attacks relating to the vCare port and protocol ingress and egress connectivity to the MFPs on the network.

Certain specifics of the vulnerability testing conducted were omitted from this document as we did not want to provide someone the information needed to abuse SMTP or POP3 services. We did wish to provide for the purpose of education and awareness sufficient detail to assist administrators in hardening their network environments.

For most secure deployments, vCare supports one way communications (push only) using SMTP and secure HTTP/HTTPs. These configurations are advisable for the most security conscious enterprise customers. However no vulnerabilities were discovered in the two-way communications methods supported by vCare while conducting this security assessment.

During a hands-on testing analysis explained in this white paper, Miercom found vCare to be a secure device relationship management system that enables uptime management of network multifunction printers and copiers. Based on an extensive security vulnerability analysis of the complete vCare system, Miercom believes vCare can be installed without compromising the security of a customer's network.

The uptime management benefits of utilizing vCare are tremendous. The system maximizes MFP uptime through real-time service alerts. Real-time email alerts were observed for critical events such as a cooling fan failure in the device. For example, the bizhub C253 has 130 specific trouble codes that it can report. The number of trouble codes and corresponding trouble counters reported by vCare is specific to each model.

Miercom recommends customers to employ a layered active security defense to any network. The deployment of vCare on a customer's network is a recommended option to aid with device uptime management. The requirements to use the system should not concern even the most security conscious customers.

2.0 Terminology Used in this Document

Attack Vector — a vulnerability test type targeting a specific area of protocol, port or other focused area to attack.

Certified Secure — Miercom's Certified Secure testing certification is a program started in 2001 that established the industry's first product and technology agnostic approach to security testing. Certified Secure Testing involves the complete system or solution for a product or service being tested using an arsenal of vulnerability security targets.

Denial of Service (DoS) — a malicious or inadvertent disruption of a network which renders it unusable or diminished in functionality during the period of the attack.

Multifunction Printer (MFP) — a network device that offers many functions, including but not limited to, network copying, fax, scanning and other functions consolidated in one device.

Mutations — a variation of an attack vector in which the data is manipulated (payload information is mutated) in order to bypass security countermeasures that employ pattern recognition technology.

Post Office Protocol (POP3) —protocol used to retrieve email from a server. Most email applications use the POP3 protocol. POP3 email is commonly critiqued for lack of security if not implemented correctly. POP3 is used to retrieve or "pull mail" whereas SMTP is used to "push" mail to external mail servers when POP3/SMTP are used in conjunction to one another.

Security Target (ST) — a set of security requirements and specifications used for testing products.

Simple Mail Transfer Protocol (SMTP) — is the foundation of Internet email. SMTP used in conjunction with a mail client application is used to send and retrieve mail.

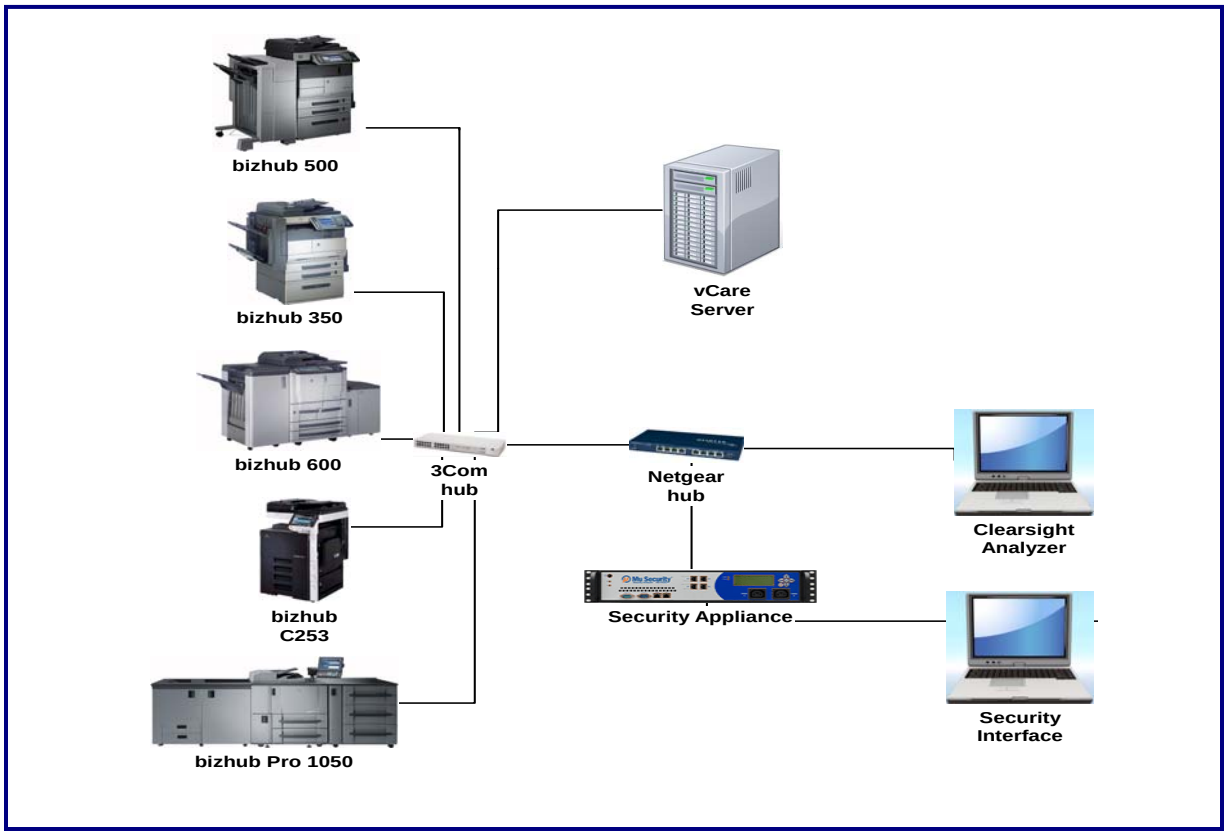
System Under Test (SUT) — Alternatively referred to as a Target of Evaluation (TOE) in other publications. An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

3.0 Testing Methodology

Miercom used a combination of custom, proprietary, commercial, and open source tools when conducting this security assessment. The test bed consisted of Konica Minolta multiple multifunction printers (MFPs) connected to a network with no security countermeasures employed. We would never expect or recommend such an unsecure environment for customer deployment, however it provides the ideal "worst case" scenario for assessing security vulnerabilities.

Test systems included ClearSight Analyzers, open source test scripts, and a Mu Security 4000 Analyzer. The ClearSight Analyzer was used to monitor and capture POP3 and SMTP traffic between the bizhub MFPs and the vCare server. Sequences of normal status and maintenance traffic as well as manually induced fan failures and recovery alert conversations between the bizhub MFP and vCare server -- in both encrypted and unencrypted mode -- were captured and analyzed to determine what sensitive information might be revealed by eavesdropping.

3.1 Test Bed



4.0 Overview of vCare

bizhub vCare is Konica Minolta's Device Relationship Management (DRM) System which consists of embedded technology within the Konica Minolta MFP and an off-site vCare Server.

Through brief email messages, the vCare-enabled MFP communicates diagnostic and counter information as requested by the vCare Server. bizhub vCare works in the background and never interferes with the operation of the MFP.

bizhub vCare enhances the customer experience in four ways:

1. Automatically reads the meters and frees the customer from the meter collection process.

2. Improves availability of the bizhub product by providing intelligent supply notifications to the customer to alert them when a specific toner is almost empty, is empty; when the waste toner bottle is almost full, is full, etc.

3. Improve machine uptime through real-time service alerts.

4. Utilizes the machine performance information collected by vCare to deliver proactive service.

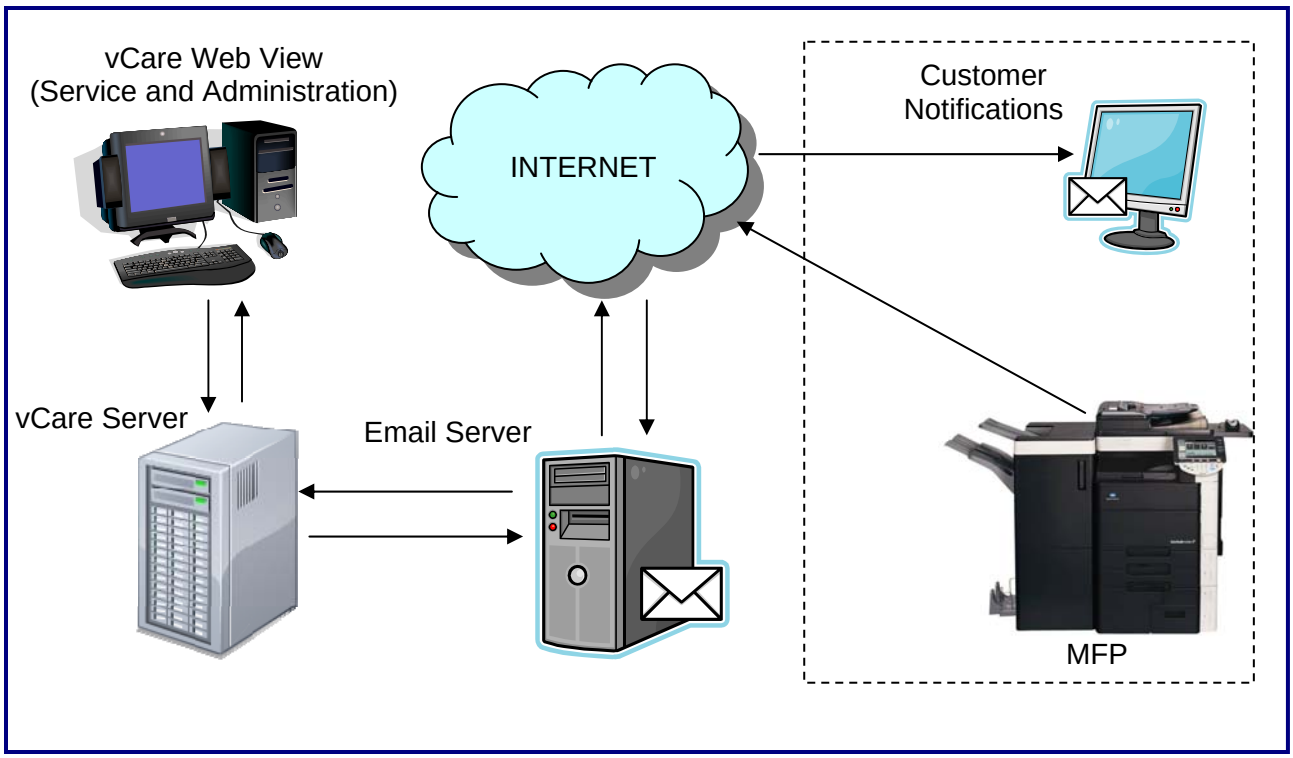
vCare provides maximum uptime of network equipment by enabling preemptive order replacement of wearing components and supplies before they run out.

Konica Minolta vCare is an environmentally friendly solution that reduces the need for service visits and unnecessary travel to equipment in the field.

5.0 Overview of vCare Email Communication Methods

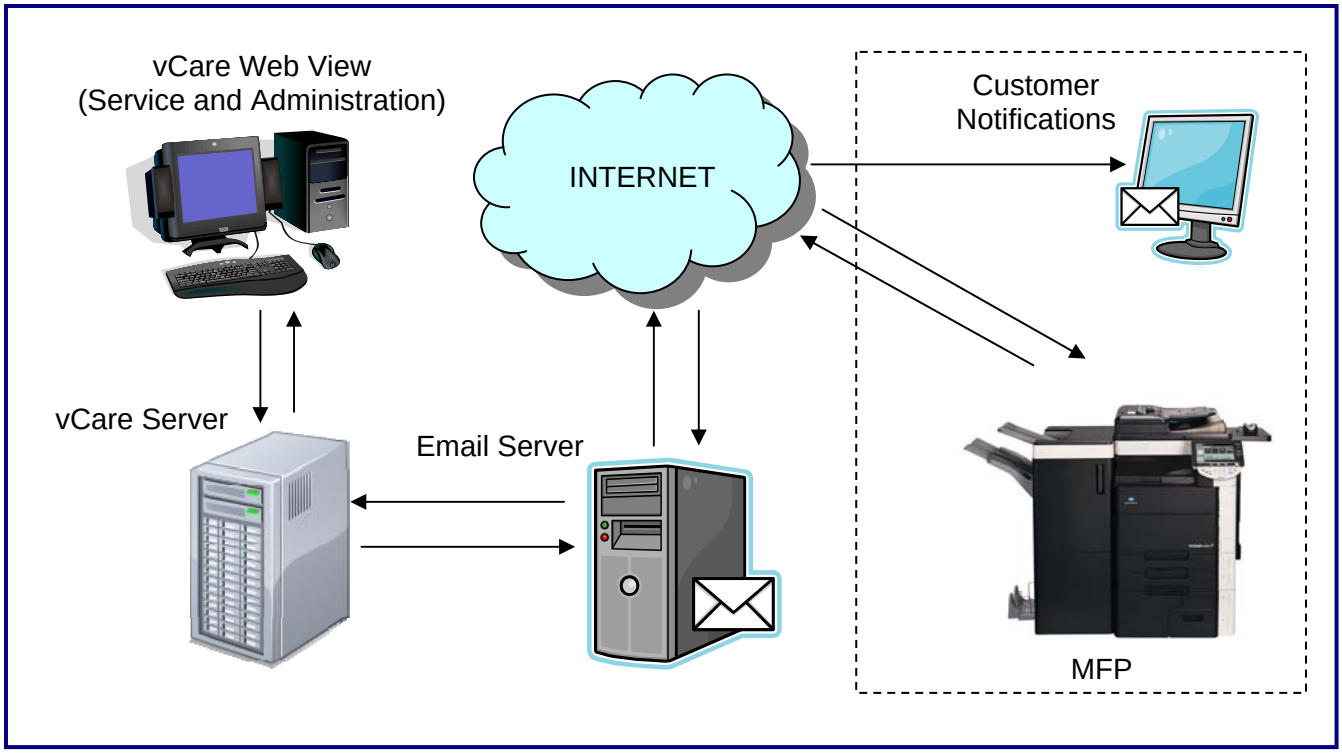
Konica Minolta multifunction printers support four methods to communicate embedded technology within the Konica Minolta MFP and an off-site vCare Server: 1) POP3 retrieval and SMTP push email; 2) SMTP push email only; 3) Secure HTTP/HTTPs push, and
4) Secure HTTP/HTTPs. These methods are illustrated in the following diagrams:

5.1 vCare One-Way Email Communication



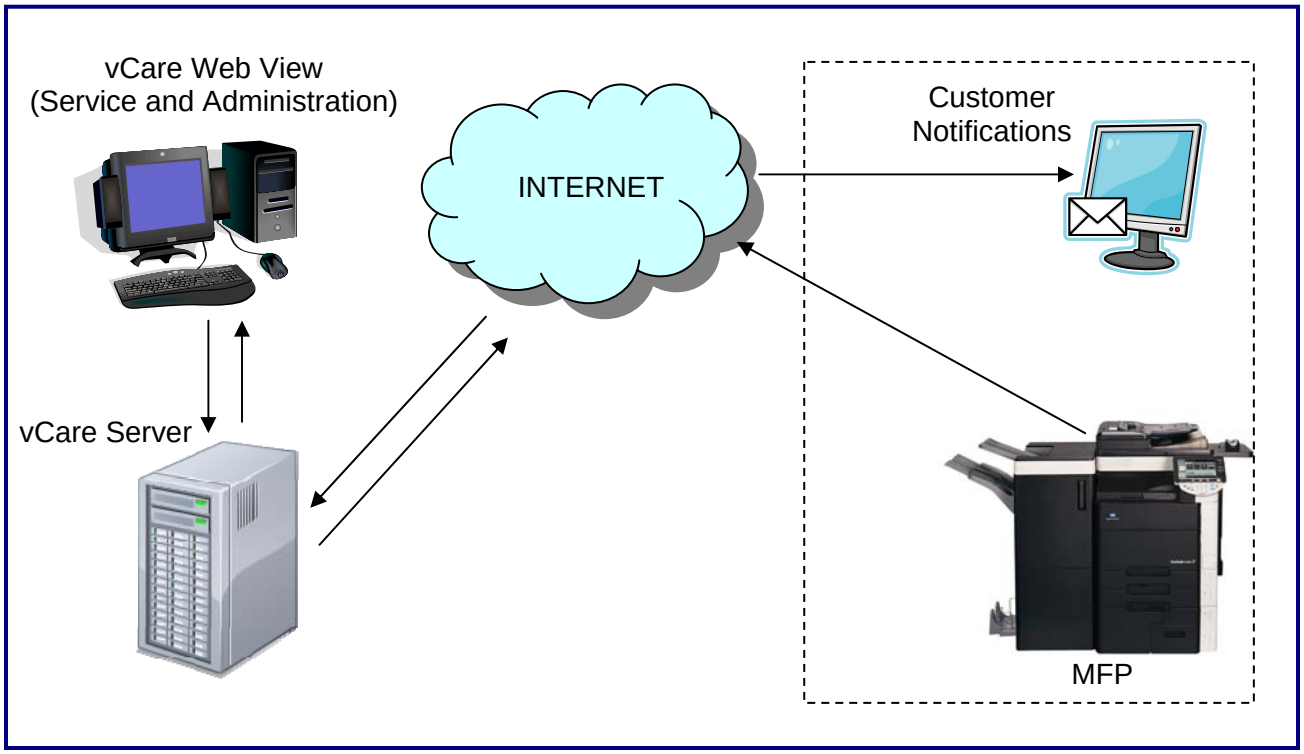
One-Way Email Communication is initiated from the bizhub MFP to send information, such as counter status, once a day to the vCare server. SMTP push is also used to send all alert notifications to predesignated email accounts via the vCare server.

5.2 vCare Two-Way Email Communication



Two-Way Email Communication allows the bizhub MFP to poll the vCare server for requests for counter status. SMTP push is also used to send these status messages, as well as alert notifications, to predesignated email accounts via the vCare server.

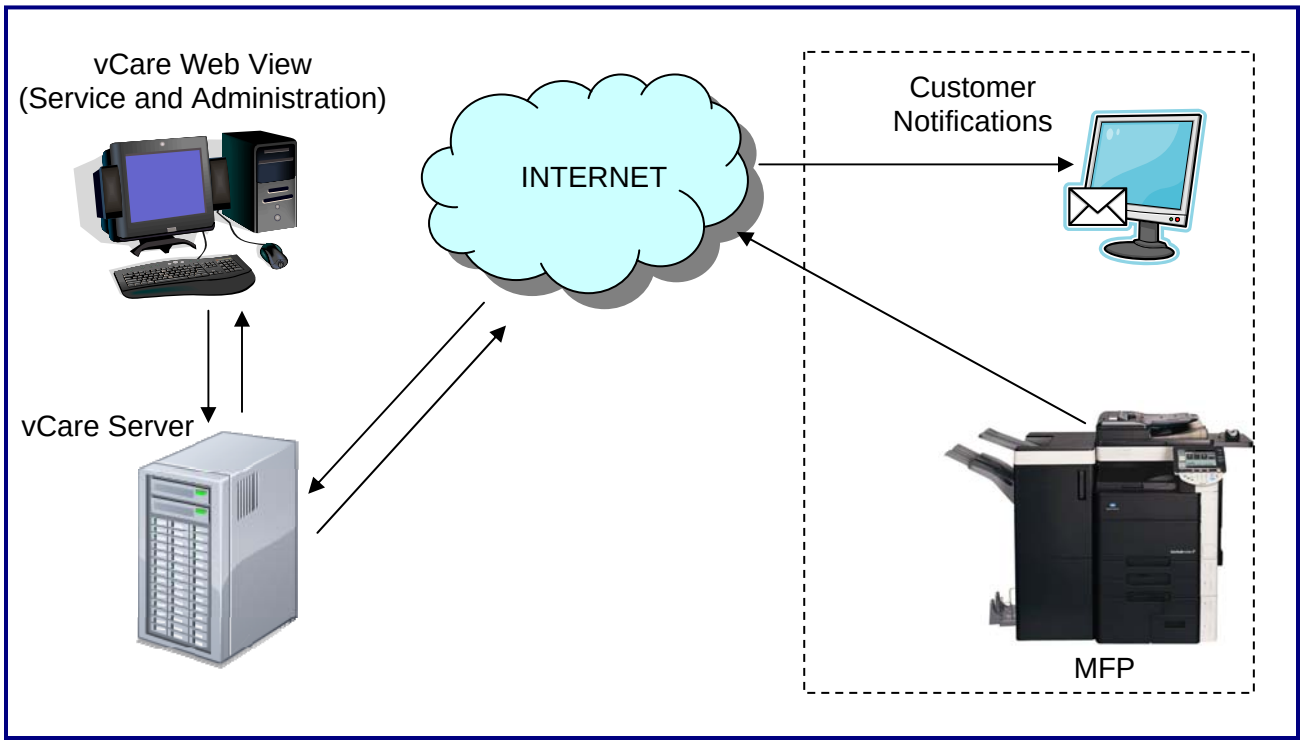
5.3 vCare One-Way HTTP/HTTPs Communication



One-Way HTTP/HTTPs Communication is initiated from the bizhub MFP to send information, such as counter status, once a day to the vCare server. HTTP/HTTPs push is also used to send all alert notifications to the predesignated vCare server.

Although HTTPs tested favorably by Miercom, the ability for Konica Minolta to support it through their infrastructure service is under development.

5.4 vCare Two-Way HTTP/HTTPs Communication



Two-Way HTTP/HTTPs Communication allows the vCare server to initiate communications to the bizhub MFP to request information, such as counter status, and report back to the vCare server. HTTP/HTTPs push is also used to send all alert notifications to the pre-designated vCare server.

Although HTTPs tested favorably by Miercom, the ability for Konica Minolta to support it through their infrastructure service is under development.

6.0 Security Assessment of the vCare-enabled MFP's vulnerability from OUTSIDE the customer's firewall - MFPs utilizing POP3/SMTP email and HTTP/HTTPs

Miercom conducted a series of vulnerability analyses and attacks in the same way a hacker would attempt to gain unauthorized access or deny use of network resources.

We found the POP3, SMTP, and HTTP/HTTPs implementation of the vCare service particularly robust and resistant to hacking from outside the network, based on hands-on testing for the following reasons:

1. The vCare system utilizes an external mail server and does not rely on or reveal any information regarding the customer premise mail server.
2. It is very unlikely that open ports for SMTP, POP3 or HTTP/HTTPs could be used as access points to a customer's private network if a properly configured firewall is implemented. Following standard practices for firewall configuration and suggestions included in this document will alleviate this threat.
3. The information contained within the payload component of the email messages can be encrypted by the MFPs' communications to and from the vCare servers. We confirmed by traffic capture that no useful intelligible data could be utilized from the encrypted data.
4. The pre-encrypted information content transmitted by the MFPs to and from the vCare servers is of no use to a hacker to gain insight to the interior network. Basic statistics, counter information and non-sensitive details on the copier's health is the only information contained within these messages.
5. Three levels of protection are provided on messages between the vCare server and the MFP, including proprietary header, proprietary attachment file and predefined source and destination addresses.
6. The basic information for copier health mentioned above can only be determined through decodes using Konica Minolta's proprietary procedure of the DAT file types.
7. Email messages to and from vCare servers are handled in a proprietary way that can reside transparently on a customer's network with no interaction whatsoever of the customer's premise mail server.
8. "Spoofing" for other malicious use of this mail component of vCare to do harm to customer premise equipment of the underlying network was found ineffective in our real world testing.

6.1 Can opening the customer's firewall to POP3 be a conduit for attacks on the network?

POP3 email hacking, in its most common form, is used to either access mail accounts or to spoof legitimate user accounts (unauthorized send on behalf of) and send messages that may flood a network or overwhelm a mail server. A properly-configured, firewalled network with mail filtering systems installed alleviates this threat.

It is extremely unlikely for a hacker to utilize POP3 as a network ingress point, with the exception of installing or packaging malicious code (to provide this entry point) in the payload or attachment component of the mail message. We tested specifically for this vulnerability and found the implementation of the vCare service using email to be extremely resilient to “piggy-back” or “Trojan” access vulnerability to a network. The following explains why we feel Konica Minolta’s implantation of POP3 is secure:

1. Tests were conducted in which we attempted to send malicious content using the POP3 mail handling component of vCare. These attacks were thwarted by the vCare server and content was not delivered to the server message blocks (SMBs) or anywhere onto the customer’s protected network.

2. We were unable to compromise the POP3 mail handling system of vCare in any way that would allow a malicious attack directly through a firewalled environment.

3. Konica Minolta uses a very defined, finite, and securable email dialog for the POP3 service it utilizes. This allows a network administrator to very easily provide a limited POP3 service to traverse the customer firewall without need to open POP3 globally.

6.2 Steps for the CUSTOMER to mitigate risk to POP3 implementation

1. Using different (non standard) port numbers for a customer's own POP3 mail is recommended if POP3 is utilized on their own servers. vCare will not employ any of the customer premise mail servers. However, if port access is opened to SMTP or POP3 through the customer's firewall, measures can be taken to ensure the customer’s mail servers (unrelated to vCare) are hardened.

2. Follow the vendor’s instructions for hardening firewalls by opening only ports that are necessary.

3. If the only POP3 access to the network is for vCare, additional filters for source and destination address, specific content filtering and other techniques may be applied to restrict other POP3 unauthorized traffic.

4. Encrypt communications using SSL to protect network traffic.

5. Utilize Konica Minolta's bizhub products that support SMTP push-only technology, if the customer is decidedly against using POP3 access through their firewall.

6. From inside the LAN, use an internal firewall to protect against accidental breaches or malicious attacks. Front-end servers can be secured by placing them inside a perimeter network (called a demilitarized zone [DMZ]), with the back-end server inside the inner firewall.

7. Again, although vCare will not utilize the customer premise mail server, the customer may still wish to harden their own mail server from attack. A common attack by flooding the mail server with mail to cause a Denial of Service can be prevented by using a number of restrictions and limiting techniques including:

    - CONNECTION RATE THROTTLING — The number of connections the server can receive per second. Setting a limit on this number can delay further connections.

    - MAX DAEMON CHILDREN — The maximum number of child processes that can be spawned by the server.

    - MIN FREE BLOCKS — The minimum number of free blocks which must be available for the server to accept mail.

    - MAX HEADERS LENGTH — The maximum acceptable size (in bytes) for a message header.

    - MAX MESSAGE SIZE — The maximum acceptable size (in bytes) for any one message.

8. Follow procedures outlined later in the document for mitigating risk for SMTP regarding firewalls and other network hardening measures.

7.0 Security Assessment of the vCare-enabled MFP's vulnerability from OUTSIDE the customer's firewall - MFPs utilizing SMTP email

Like many other tools, SMTP can have a dark side. This is mainly due to the fact that, as you'd expect from something with the word "simple" in its name, SMTP is simple to install and use.

Because of that, SMTP email, like POP3 email hacking in its most common form, is often improperly used to access mail accounts or spoof (unauthorized send on behalf of) messages that may flood a network or overwhelm a mail server. The key is creating good policies for SMTP's use on networks. A properly configured firewalled network with mail filtering systems installed alleviates this threat.

7.1 Can opening the customer's firewall to SMTP be a conduit for attacks on the network?

It is highly unlikely a hacker would choose to use SMTP as a network ingress point except for installing malicious code in the payload or attachment part of a mail message. During our tests, we found the vCare service to be highly resilient to Trojans or other ingress points for network attack. Even with the low risk to attack by opening ports to SMTP, the following are steps that a customer could take to further harden the network environment.

7.2. Steps for the CUSTOMER to mitigate risk when implementing SMTP email systems

1. Reduce the number of gateways that are allowed to communicate via SMTP on the Internet to only those required. All processes that must send email should be allowed to forward it only through an authorized gateway.

2. Administrators should establish firewall rules that allow only authorized gateways to communicate with outside servers on TCP ports 25 or 465.

3. Again, although vCare will not utilize the customer premise mail server, the customer may still wish to harden their own mail server from attack if ports are opened for SMTP access through the customer premise firewall. To help stop attackers from speaking SMTP directly to a full-featured server, experts recommend using a substitute server. Only a handful of commands are needed by an SMTP server to accept mail. A few ways to mitigate this risk are outlined below:

    a. Use a substitute SMTP server - consider using smap, if you have a Linux/Unix based server, as a "wrapper" for your SMTP server. Wrapper or mail proxy programs accept incoming messages from the Internet via SMTP, using the very minimum necessary set of SMTP

commands. It then stores each message it receives in a separate file that is then accessed by the primary mail server. The result of using this substitute SMTP server is that a hacker never has a direct SMTP connection to the primary mail server.

b. Test your firewall - you can test your firewall rules to ensure they are working properly. We recommend scanning tools for this purpose. Some recommended all-in-one tools that allow for broad testing capabilities that make the network scanning process less painful and time consuming: *Nessus, QualysGuard, NetCat, Traffic IQ Pro* by Karalon, and *GFI LANguard Network Security Scanner*. These tools identify open ports on the test networks and present information on SNMP, operating system, and special alerts.

4. Countermeasures against firewall attacks - the following countermeasures can prevent a hacker from testing the firewall

   a. Limit traffic - set rules on the firewall or router to allow authorized traffic. Have permission/rules in place for external access that allows only specified inbound and outbound traffic. This is the best defense to prevent an attack on the firewall.

   b. Block ICMP to help prevent abuse from automated tools, such as Firewalk.

   c. Stateful packet inspection on the firewall can block unsolicited requests.

8.0 Security Assessment of the vCare-enabled MFP's vulnerability from INSIDE the customer's firewall - MFPs utilizing POP3 or SMTP email.

In the event of a hacker successfully infiltrating the firewall and other network defenses and having gained access to the network, a second level of security countermeasures are needed to protect resources inside the network. A layered defense, rather then an all-in-one solution, with a strong external firewall is required. Once inside the firewall, it is easy to see the passwords for POP3 email accounts in the clear. This allows for logging into the POP server to get mail, since unencrypted usernames and passwords appear on the network. The use of Web forms that contain usernames and passwords can also expose usernames and passwords.

The primary vulnerability seen from within the network regarding POP3 is the potential access to the email accounts themselves.

SMTP service is always a “push” sending email out from the MFPs off the customer network. There is little to no risk from inside the network from an SMTP standpoint.

8.1 Can opening the customer's firewall to POP3 be a conduit for attacks on the network?

Using techniques described previously in this document for network and email server hardening will mitigate this risk. Hands-on vulnerability testing that Miercom conducted with “privileged” local access could only disrupt the vCare management system. We could not conduct further attacks on the network using POP3. The mail server for POP3 is located off the customer premise. We were unsuccessful as previously discussed using POP3 as a means to provide a greater DOS attack.

8.2 Protocol Mutation test against vCare server

Protocol mutation attacks created by the Mu-4000 Service Analyzer were directed at the Konica Minolta vCare server to test for vulnerabilities in protocol implementation. The mutation engine maps the attack surface (vCare server) looking for fault conditions. These include highly specific, stateful test cases that are built based on the state, structure and semantics of protocols as well their interdependencies on other protocols.

Test

The HTTP/HTTPs mutation attack was run with 11,135 different variants. Each variant/attack vector carried a single protocol mutation directed to the vCare server. We sent mutated HTTP/HTTPS requests to the vCare server once we achieved a TCP connection.

Observations

All directed attacks to the vCare server were handled successfully and no faults were found. The vCare server was available for the duration of the test. There were no vulnerabilities detected with HTTP/HTTPs protocol implementation on the vCare server.

8.3 Steps for the CUSTOMER to mitigate risk inside the network

Although vCare poses no additional risk to customer networks, Miercom recommends implementing intrusion detection technologies and switching equipment that employs rate limiting and other DoS thwarting measures on any network.

9.0 Conclusion

"Konica Minolta offers the market the most resilient and secure MFP solutions with exceptional uptime management. Konica Minolta is the only vendor to date to have achieved Miercom Certified Secure for a third consecutive year for the multifunction printer products with uptime management provide by vCare Device Relationship Management System."

--- Rob Smithers, CEO Miercom

vCare is a secure device relationship management system that enables uptime management of network multifunction printers and copiers. Based in extensive security vulnerability analysis of the complete vCare system, Miercom believes vCare can be installed without compromising the security of a customer's network.

The reasons that the vCare solution does not pose a security risk to a customer's network:

1. Information that is transferred using vCare is of no significant use to a hacker.
2. Three layers of security are employed on all email messages used for vCare.
3. An SMTP push only for sending information off net requires no inbound network security access reconfiguration
4. Management option available through secure HTTP/HTTPs; also through "push only" default option for maximum security.

Miercom conducted a battery of assaults to disrupt the multifunction printers using vCare. We were unsuccessful in hacking into the bizhub solutions through the network ports and unable to affect the ability of the multifunction printers to print, be managed, or actively participate in vCare reporting by any attacks through the vCare functionality. HTTPs tested favorably although the ability for Konica Minolta to support it through their infrastructure is under development.

The uptime management benefits of utilizing vCare are tremendous. The system maximizes MFP uptime through real-time service alerts. Real-time email alerts were observed for critical events, such as a cooling fan failure in the device, and, depending on the model, there are over 100 trouble counters supported.

Miercom recommends customers to employ a layered active security defense to any network. The deployment of vCare on a customer's network is strongly encouraged as an aid with MFP device uptime management. We see no risk and only many benefits of implementing vCare in customer environments. The requirements to use the system should not concern even the most security conscious customers.

About Miercom

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including *Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony* and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services 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 NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.

This report is available for download at http://www.miercom.com/konicaminolta