Miercom

Security White Paper

DLR 110623

Konica Minolta CS Remote Care (CSRC) with E-mail, HTTP, GSM, GPRS and fax modems

Device Relationship Management System

June 2011

Miercom
www.miercom.com

Contents

Executive Summary

Multifunctional printers (MFPs) from Konica Minolta with uptime management provided by CS Remote Care (Marketed worldwide as CSRC, bizhub vCare, Sentinel Archange, and Digital Doctor) Device Relationship Management System proved during thorough lab testing and onsite assessment, to provide superior resiliency and resistance to network compromise and achieved Miercom Certified Secure for the fourth consecutive year.

Miercom tested the overall security of Konica Minolta's GSM, GPRS and fax modems complete with device relationship management system KM CS Remote Care (CSRC) and the bizhub C550, bizhub 652, bizhub 501 and bizhub C6000 multifunction printers (MFPs). The modems were tested as a complete solution while Miercom engineers assessed the dialog between the CSRC Service Center and the MFPs for potential vulnerability. We evaluated the overall capability of the modems with CSRC to provide uptime management of networked MFPs. We reviewed the security of the modems, MFPs and CSRC servers for vulnerability to DoS and other specific attacks relating to the CSRC port and protocol ingress/egress connectivity to the MFPs on the network via the modems.

Certain specifics of the vulnerability testing conducted were omitted from this document to prevent providing information needed to abuse SMTP or POP3 services. Sufficient detail to assist administrators in hardening their network environments is included for educational purposes.

For most secure deployments, CSRC 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 CSRC while conducting this security assessment. CSRC also supports secure communication over GSM, GPRS and fax modems with the MFPs. In our testing, this scenario proved to be the most secure method for deployment.

During a hands-on testing analysis explained in this white paper, Miercom found CSRC 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 CSRC system, Miercom believes CSRC can be installed without compromising the security of the network.

The uptime management benefits of utilizing CSRC 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 can be reported. The number of trouble codes and corresponding trouble counters reported by CSRC is specific to each model.

Miercom recommends customers to employ a layered active security defense to any network. The deployment of CSRC on a customer 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.

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 — a Miercom program started in 2001 that established the 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 with diminished functionality during the attack period.

Multifunction Printer (MFP) — a network device offering 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. 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. POP3/SMTP are often used in conjunction with 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 sends and retrieves mail.

System Under Test (SUT) — a product or system that is the subject of an evaluation.

Global System for Mobile (GSM) – GSM is a standard set developed by the European Telecommunications Standards Institutes (ETSI) to describe technologies for second generation (2G) digital cellular networks.

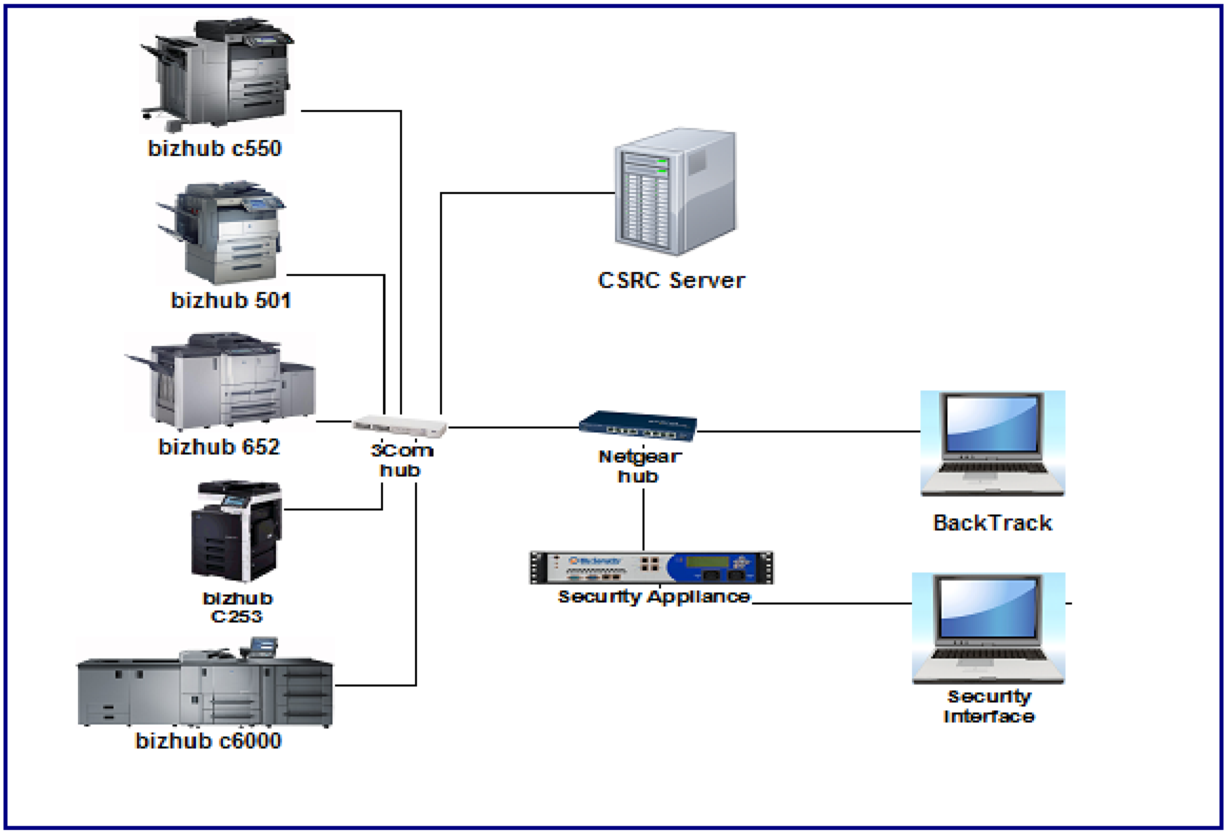
General Packet Radio Service (GPRS) – GPRS is a packet oriented mobile data service on the 2G and 3G cellular communication systems global systems for GSM.

Testing Methodology

A combination of custom, proprietary, commercial, and open source tools was used to conduct this security assessment. The test bed consisted of Konica Minolta multiple multifunction printers (MFPs) connected to a network without any security countermeasures employed. This environment is not recommended for a customer deployment; however it provides the ideal “worst case” scenario for assessing security vulnerabilities.

Test systems included ClearSight Analyzer, BackTrack, 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 CSRC server. Sequences of normal status and maintenance traffic as well as manually induced fan failures and recovery alert conversations between the bizhub MFP and CSRC server -- in both encrypted and unencrypted mode -- were captured and analyzed to determine what sensitive information might be revealed by eavesdropping. Zenmap was used to scan open ports on each of the MFPs and communication server.

Test Bed Diagram



Overview of CSRC

CS Remote Care is the Device Relationship Management (DRM) System which consists of embedded technology within the Konica Minolta MFP and an off-site CSRC Server.

Through brief communication messages, the CSRC-enabled MFP communicates diagnostic and counter information as requested by the CSRC Server. CS Remote Care works in the background and does not interfere with the operation of the MFP. This capability is possible by utilizing a modem installed on the MFP, operating separately from the customer network. These modems can be GSM, GPRS or fax.

CS Remote Care 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 to toner status, waste toner bottle status, and other supply related information.

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

4. Utilizes the machine performance information collected by CS Remote Care to deliver proactive service.

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

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

Overview of CSRC Email Communication Methods

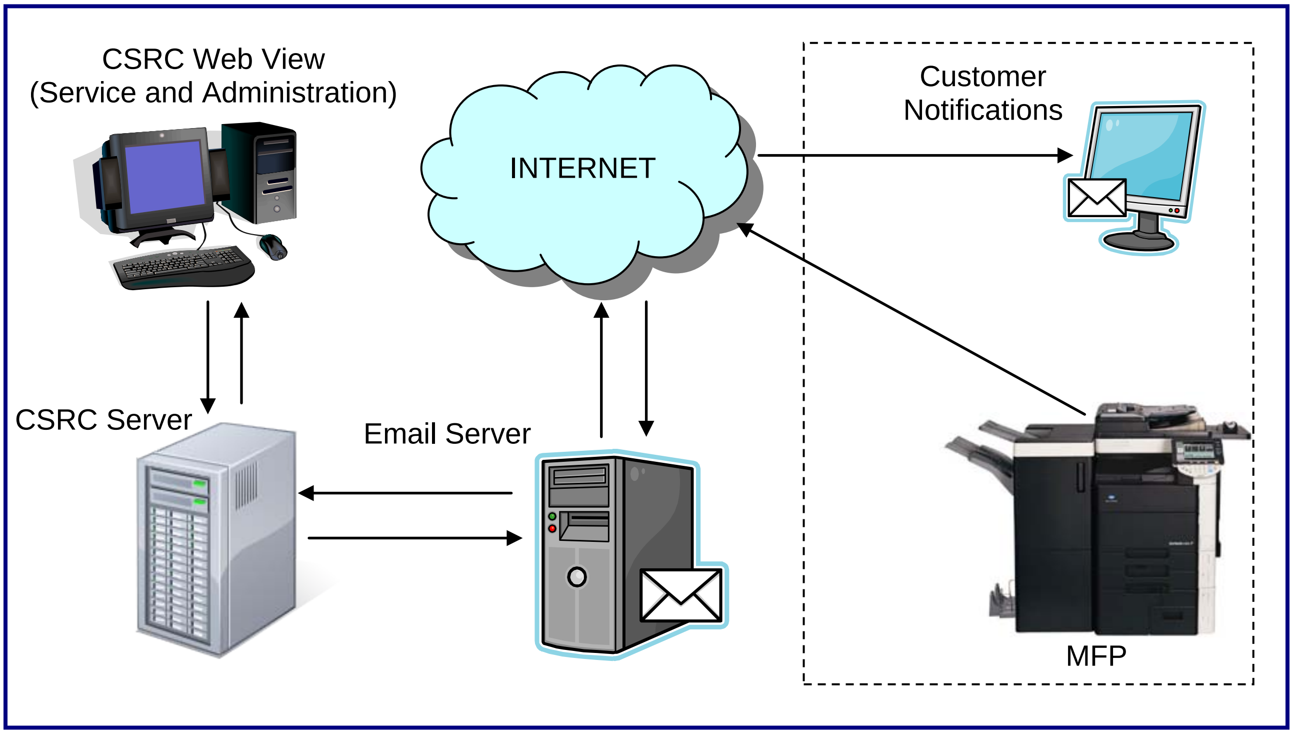
Konica Minolta multifunction printers support four methods to provide communication between the MFP and off-site CSRC Servers. This is embedded in the Konica Minolta MFP.

POP3 retrieval and SMTP push email
SMTP push email only
Secure HTTP/HTTPs push
Secure HTTP/HTTPs

The MFPs can also communicate with the CSRC server using three different types of modems: GSM, GPRS or Fax modems.

The following diagrams illustrate several methods of communication:

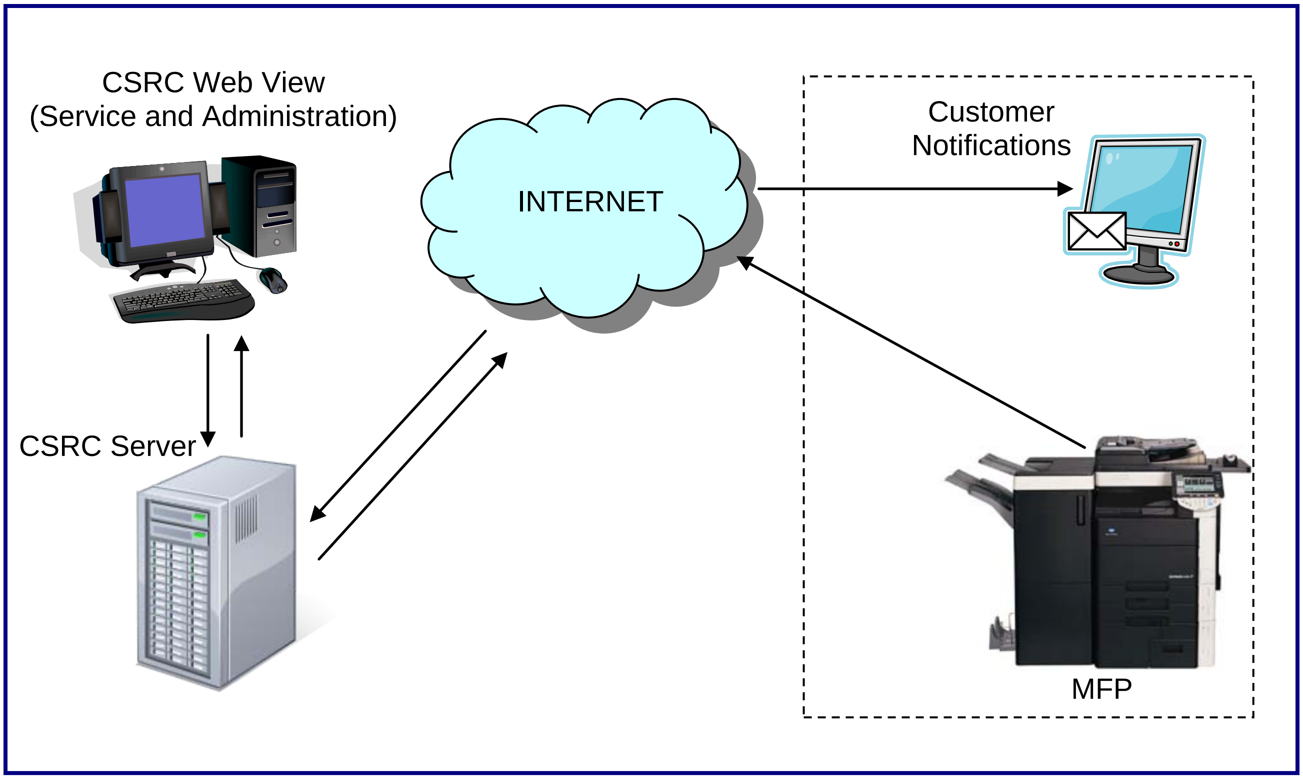
CSRC One-Way and Two-Way Email Communication



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

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

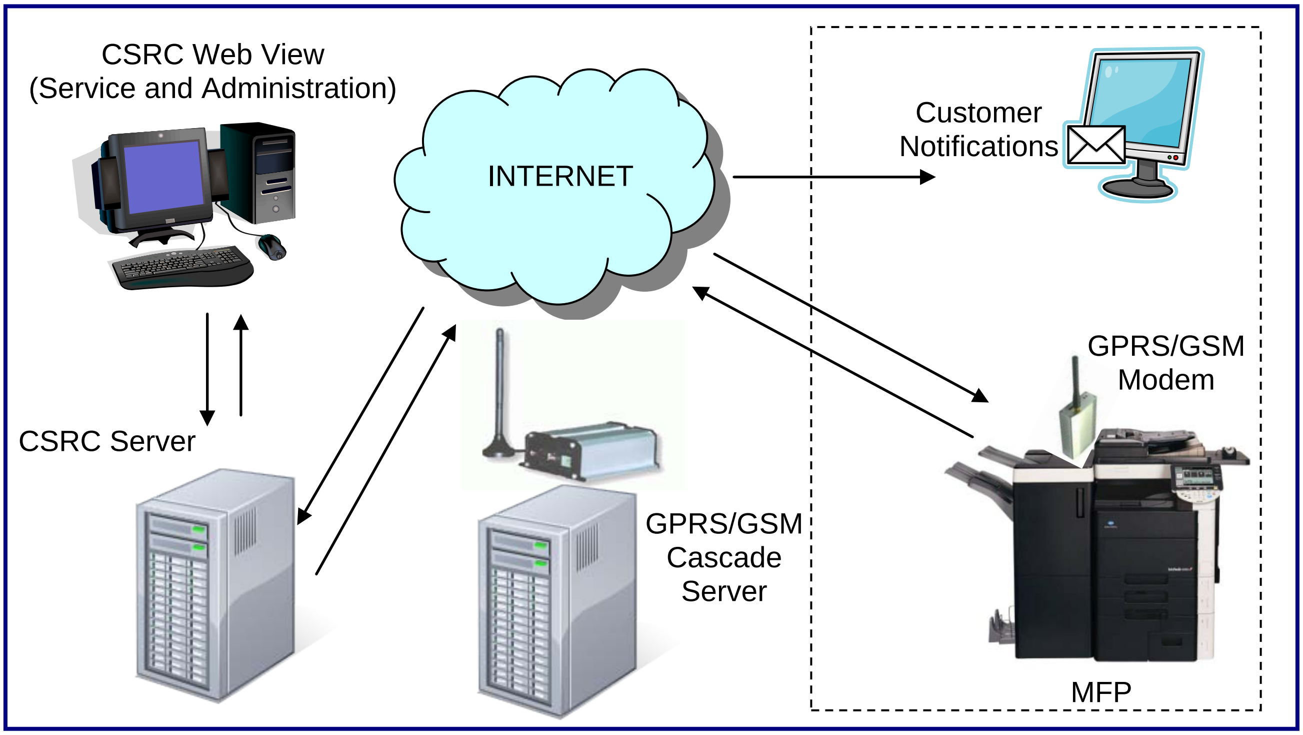
CSRC One-Way and Two-Way HTTP/HTTPs Communication



One-Way HTTP/HTTPs communication is initiated from the bizhub MFP to send information, such as counter status, daily to the CSRC server. HTTP/HTTPs push is also used to send all alert notifications to the predesignated CSRC server.

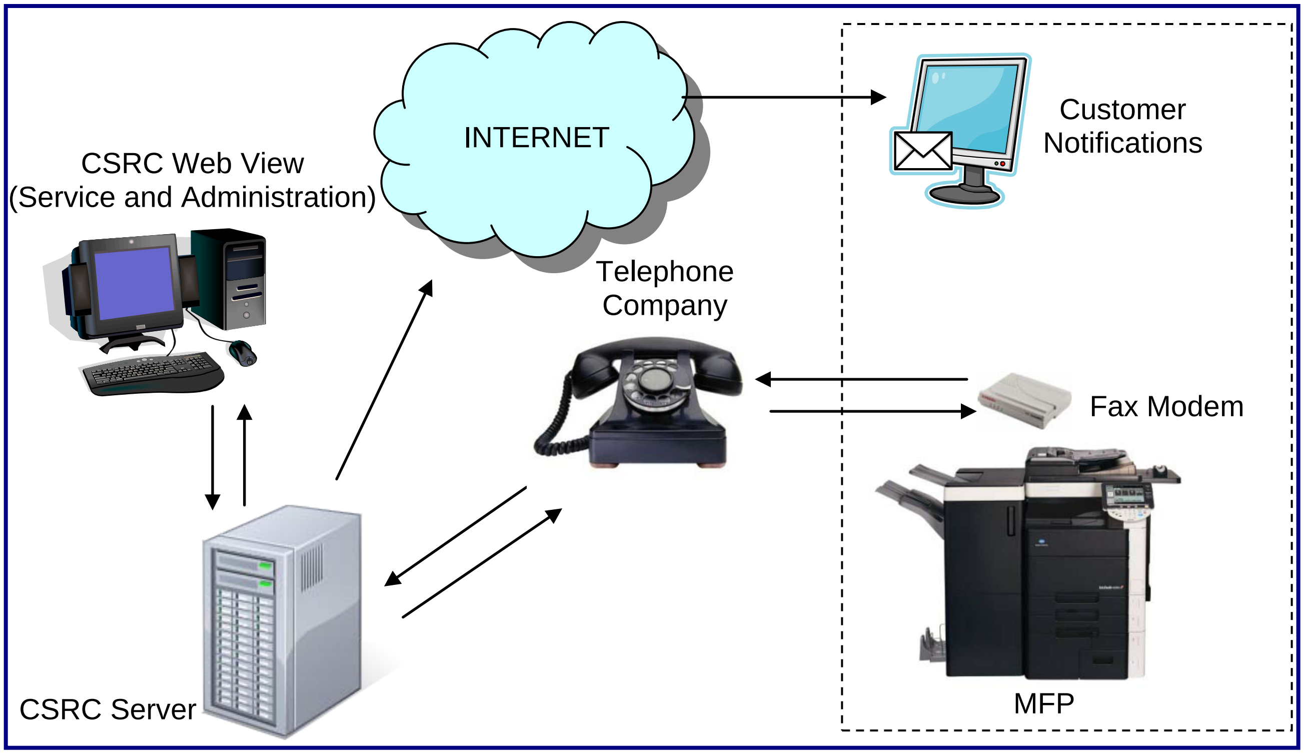
Two-Way HTTP/HTTPs communication allows the CSRC server to initiate communications to the bizhub MFP to request information, such as counter status, and report back to the CSRC server. HTTP/HTTPs push is also used to send all alert notifications to the pre-designated CSRC server. CSRC Two-Way Modem Communication.

GPRS/GSM Two-Way Communication



Two-Way GPRS/GSM communication allows the CSRC server to initiate communications to the bizhub MFP to request information, such as counter status, and report back to the CSRC server. Unlike HTTP/HTTPs and Email communication, GPRS/GSM allows communication with the CSRC server directly, completely bypassing the customer network for maximum security.

Fax Two-Way Communication



Two-Way Fax communication works the same way as GPRS/GSM communication by using a fax modem. The CSRC server can initiate communications to the bizhub MFP to request information, such as counter status, and report back to the CSRC server. Fax also communicates directly with the CSRC server, bypassing the customer network, eliminating any security risks.

Security Assessment

Vulnerability from outside firewall using POP3/SMTP; HTTP/HTTPS; GPRS/GSM/fax modems

A series of vulnerability analyses and attacks were deployed 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 either over the customer network or over GPRS, GSM and fax to be particularly robust and resistant to hacking from outside the network, based on hands-on testing. The following are specific reasons:

1. The CSRC system utilizes an external mail server and does not rely on or reveal any information regarding the customer premise mail server.
2. With a properly configured firewall at the customer site, open ports for SMTP, POP3 or HTTP/HTTPs are unlikely to be used as access points to a private network. Following standard practices for firewall configuration and other 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 CSRC 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 CSRC 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 is the only information contained within these messages.
5. Three levels of protection are provided on messages between the CSRC server and the MFP, including proprietary header, proprietary attachment file and predefined source and destination addresses.
6. The basic information for copier health can only be determined through decodes using a Konica Minolta proprietary procedure of the DAT file types.
7. Email messages to and from CSRC servers are handled in a proprietary way that can reside transparently on a customer network with no interaction whatsoever of the customer premise mail server.
8. "Spoofing" for other malicious use of this mail component of CSRC to do harm to customer premise equipment of the underlying network was found ineffective in our real world testing.
9. A hacker cannot gain access to the GPRS, GSM or fax modems to disrupt communication between the MFP and the CSRC server. Traffic between the MFPs and the CSRC server are secured by completely bypassing the customer network, communicating directly with Konica Minolta servers through GPRS, GSM or fax.

Can opening the 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 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 specifically tested for this vulnerability and found the implementation of the CSRC service using email to be extremely resilient to “piggy-back” or “Trojan” access to a network. Konica Minolta’s implantation of POP3 is secure based on the following observations:

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

2. We were unable to compromise the POP3 mail handling system of CSRC 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 easily provide a limited POP3 service to traverse the customer firewall without need to open POP3 globally.

Steps to mitigate risk to POP3 implementation

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

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

3. If the only POP3 access to the network is for CSRC, 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 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. Although CSRC 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 setting a number of restrictions and limiting techniques including:

    - CONNECTION RATE THROTTLING — the number of connections the server can receive per second. Setting a limiting number can delay further connections.

    - 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 on page 13 for mitigating risk for SMTP regarding firewalls and other network hardening measures.

Security Assessment

Vulnerability from outside firewall using SMTP email

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 to prevention is to create good policies for using SMTP on networks. A properly configured firewalled network with mail filtering systems installed alleviates this threat.

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 CSRC 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 additional steps a customer could take to further harden the network environment.

Steps 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. CSRC 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, we 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. Each message it receives is stored in a separate file that is accessible by the primary mail server. This substitute SMTP server prevents a hacker direct access to SMTP connection to the primary mail server.

b. Test your firewall - 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 are: *Nessus, QualysGuard, NetCat, Traffic IQ Pro* by Karalon, and *GFI LANguard Network Security Scanner*. These tools identify open ports on the networks and present information on SNMP, operating system, and other special alerts.

Countermeasures can prevent a hacker from accessing 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.

Security Assessment

Vulnerability from inside firewall using POP3 or SMTP

In the event a hacker successfully infiltrated the firewall and other network defenses and gained access to the network, a second level of security countermeasures are recommended to protect resources inside the network. A layered defense, rather than an all-in-one solution, with a strong external firewall is required. Once inside the firewall, passwords for POP3 email accounts are clearly visible. Logging into the POP server to get mail, allows 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.

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

Using techniques described previously on pages 13 and 14 for network and email server hardening will mitigate this risk. Hands-on vulnerability testing conducted with “privileged” local access could only disrupt the CSRC 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 on page 11 using POP3 as a means to provide a greater DoS attack.

Steps to mitigate risk inside the network

Although CSRC 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.

Security Attacks against MFPs, CSRC server and Communication Server

Protocol mutation attacks created by the Mu-4000 Service Analyzer were directed at the Konica Minolta MFPs, CSRC server and communication server to test for vulnerabilities in protocol implementation. These attacks were also directed towards the MFPs and communication server. The mutation engine maps the attack surface (MFP, CSRC server and communication server) looking for fault conditions. These attacks 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.

Before performing these attacks we completed a Zenmap scan on each attack surface to obtain a list of open and vulnerable ports. Once the list of ports was acquired, we configured the Mu-4000 Service Analyzer to attack each device specific to its vulnerable ports.

During our security attacks on the SUTs we simulated error codes by unplugging fans on the MFPs. Each time an error code is detected on the MFP it communicated back to the CSRC server using a configured modem (GSM, GPRS or fax). This verified whether the communication between the MFP and CSRC server remained intact via the configured modems.

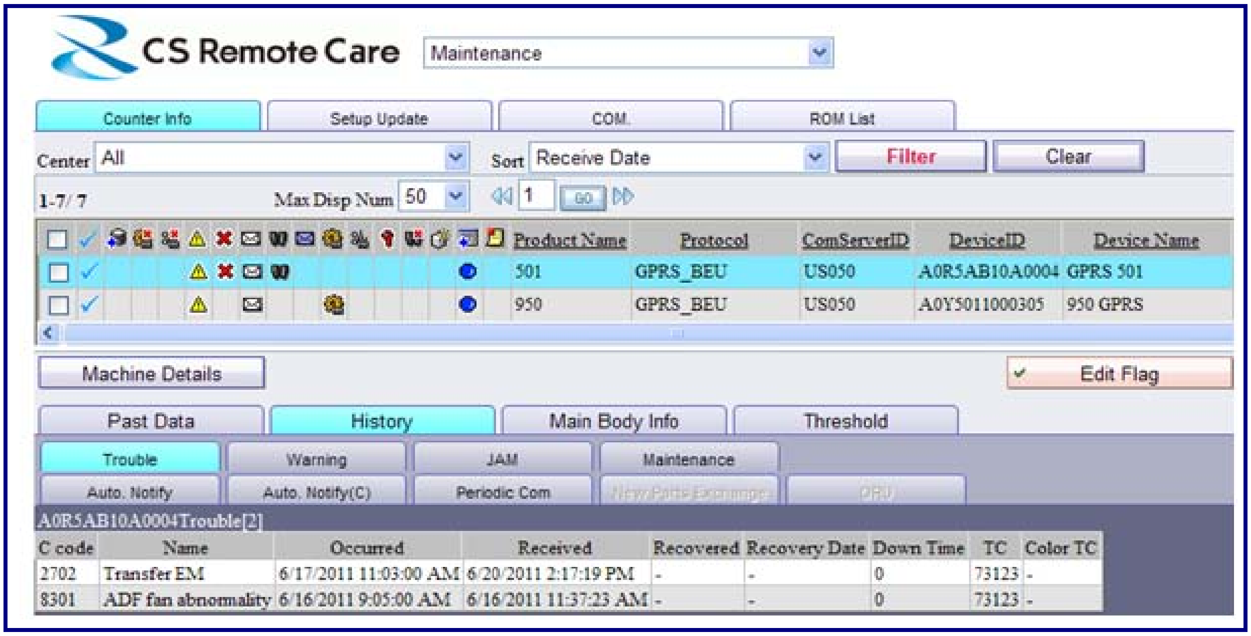
DoS Attacks – MFP, Communication Server

Denial of Service (DoS) attacks were generated and directed at the MFPs and Communication server to verify reliability, availability and security of service in the event of DoS attacks or extreme service level traffic. The DoS attack was run against the MFPs and communication server.

The first DoS attack sent 100,000 IP packets per second directed at the MFPs IP address. The second attack was directed at the communication server, also sending 100,000 IP packets per second.

This DOS attack tests the ability of the modems and server to withstand the attack and not be disrupted. Functionality of Konica Minolta CSRC system remained operational during our DoS attack on the MFP and communication server.

Fan Failure recorded in CSCR



Maintenance

Center All   Sort Receive Date

1-7/ 7   Max Disp Num 50   1

☐	✓		Product Name	Protocol	ComServerID	DeviceID	Device Name
☐	✓	⚠ ✖ ✉ ●	501	GPRS_BEU	US050	A0R5AB10A0004	GPRS 501
☐	✓	⚠ ✉ ●	950	GPRS_BEU	US050	A0Y5011000305	950 GPRS

A0R5AB10A0004Trouble[2]

C code	Name	Occurred	Received	Recovered	Recovery Date	Down Time	TC	Color TC
2702	Transfer EM	6/17/2011 11:03:00 AM	6/20/2011 2:17:19 PM	-	-	0	73123	-
8301	ADF fan abnormality	6/16/2011 9:05:00 AM	6/16/2011 11:37:23 AM	-	-	0	73123	-

During our attack we disconnected a fan from the MFP to create a fan failure. The fan failure generates a unique error code which is then sent via modem to the servers. CSRC shows the exact time of the fan failure, and also includes the time the fan error recovered.
If an attacker gains privileged access to a customer network and attempts a DoS attack on the MFP to disrupt communication it will be unsuccessful. MFP status messages back to CSRC will remain functional on all three modems tested. We saw the same results during our DoS attack against the communication server.

TCP Attack on Vulnerable ports – MFPs, CSRC server and Communication server

TCP is designed to deliver ordered streams of data from one program to another across a network. TCP is considered connection-oriented, meaning a communication session needs to be established using SYN (Synchronize) and ACK (Acknowledge) bits.

A TCP attack was run against all open ports found on the MFPs, CSRC server and Communication server. The open ports that the Zenmap port scanning application found were analyzed and attacked accordingly. The purpose of the test is to verify that all open ports are secure from TCP based attacks. This also determines if the configured modem communication is secure between the MFP and CSRC.

Our directed TCP attacks toward the open ports on the MFPs, CSRC server and communication server was unsuccessful in finding any vulnerabilities. No security flaws with the open ports have been found that would enable an attacker to obtain sensitive information. The modem communication also remained secured during our attacks and did not cause any communication outages.

HTTP/HTTPs Protocol Mutation attack against CSRC server

The HTTP/HTTPs mutation attack was run with 11,135 different variants. Each variant/attack vector carried a single protocol mutation directed to the CSRC server. Mutated HTTP/HTTPS requests to the CSRC server were sent via a TCP connection.

The Mu-4000 Security Analyzer was configured to attack the HTTP/HTTPs ports on the CSRC server. The purpose of the test is to verify that the HTTP/HTTPs ports on the server are secure and cannot be compromised and communication between the modems and CSRC server is secure.

All directed attacks to the CSRC server were handled successfully and no faults were found. The CSRC server was available for the duration of the test. There were no vulnerabilities detected with HTTP/HTTPs protocol implementation on the CSRC server. Konica Minolta HTTP/HTTPs protocol implementation on the CSRC server is highly secure. If an attacker tried to attack the HTTP and HTTPs ports on the CSRC server, the modem communication with the Konica Minolta servers will remain intact.

ARP Protocol Mutation attack against MFPs

ARP (Address Resolution Protocol) is a communications protocol used for resolving network layer addresses into link layer addresses for transmission. It is used for communication inside a network. The Mu-4000 Security Analyzer was configured to attack the ARP protocol on the CSRC server.

All directed attacks to the CSRC server were handled successfully and no faults were found. The CSRC server was available for the duration of the test. There were no vulnerabilities detected with ARP protocol implementation on the CSRC server. Konica Minolta's ARP protocol implementation on the CSRC server is highly secure. If the ARP protocol was attacked on the CSRC server, the modem communication with the Konica Minolta servers would remain intact.

DHCP Protocol Mutation attack against MFPs

DHCP is a format for transferring information from one computer or device to another in order to determine the dynamic IP address. With dynamic IP addressing each time a device connects with another or to a network, the IP address could change. The proper transfer of the IP address data is important to keep a device performing smoothly. Corruption of this data could cause a failure of the device. We tested to see whether the dynamic IP address could be corrupted by an attack from the mutated DHCP protocol.

The Mu-4000 Security Analyzer was configured to attack the DHCP protocol on the multifunction printers.

All directed attacks to the MFPs were handled successfully and no faults were found. The MFPs were available for the duration of the test. There were no vulnerabilities detected with DHCP protocol implementation on the CSRC server. Konica Minolta's DHCP protocol implementation on the CSRC server is highly secure. If an attacker tried to attack the DHCP protocol on the CSRC server, the modem communication with the Konica Minolta servers will remain intact.

Conclusion

> “Konica Minolta offers the market a most resilient and secure MFP solution with exceptional uptime management. Konica Minolta is the only vendor to date to have achieved Miercom Certified Secure for a fourth consecutive year for the multifunction printer products with uptime management provide by CS Remote Care (Marketed worldwide as CSRC, bizhub vCare, Sentinel Archange and Digital Doctor Device Relationship Management System.”
>
> --- Rob Smithers, CEO Miercom

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

CSRC solution does not pose a security risk to a customer’s network because:

- Information transferred using CSRC is of no significant value to a hacker.
- Three layers of security are employed on all email messages used for CSRC.
- An SMTP push only for sending information off net requires no inbound network security access reconfiguration
- Management option available through secure HTTP/HTTPs; also through “push only” default option for maximum security.
- MFPs communicate with Konica Minolta CSRC servers directly using GSM, GPRS or fax, completely bypassing the customer network eliminating any security risks.

Miercom conducted a battery of assaults to disrupt the communication between the multifunction printers and CSRC. We were unsuccessful in hacking into the bizhub solutions through the network ports and unable to affect the ability of the MFPs to print, be managed, or actively participate in CSRC reporting by any attacks through the CSRC functionality. We found that Konica Minolta’s deployment of GSM, GPRS and Fax modems for communication directly with their servers is a well implemented approach. In our thorough testing we could not find any type of security vulnerability in the implementation of GSM, GPRS, or fax.

The uptime management benefits of utilizing CSRC 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, supplies needed, service required, or any of over 100 other trouble counters supported.

Miercom recommends customers to employ a layered active security defense to any network. The deployment of CSRC on a customer network is strongly encouraged as an aid with MFP device uptime management. We see no risk and only benefits of implementing CSRC 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, Tech Web - 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

Konica Minolta is a trademark of Konica Minolta Holdings, Inc. bizhub is a registered trademark of Konica Minolta Business Technologies, Inc. All other trademarks mentioned in this document are the property of their respective owners.