Konica Minolta Remote Service Platform Security Assessment

January 2021

SR201222D

Contents

1.0 Executive Summary

Multi-function Printers (MFPs) are devices that allow businesses to print, copy, scan, fax and perform other tasks. Traditionally, customer care for these devices required on-site maintenance for operations, such as toner replacement and firmware upgrades. Now, customers benefit from remote services that eliminate travel, costs and downtime.

Konica Minolta helps drive productivity using an automated, cloud-based monitoring and device reporting service – Worldwide Remote Service Platform (WWRSPF, hereinafter, this is called "RSP"). Like any other network endpoint, MFP components are susceptible to threats. Miercom recommends MFP management solutions are encouraged to be as secure as possible when handling these devices. This solution optimizes maintenance operations while keeping MFPs secured.

Konica Minolta Inc. (KMI) engaged Miercom to perform a comprehensive security assessment of its Remote Service Platform and two MFP products 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.

The test scope focused on security analysis of the Remote Service Platform solution hosted via Amazon Web Service (AWS) data center. We were further commissioned to analyze the Konica Minolta WebDAV server, Remote Console server, and XMPP servers. Any communication interaction between Konica Minolta servers and Remote Service Platform were considered part of the analysis therein. We also looked at vulnerabilities affiliated with the MFP devices.

Key Findings

- Impressive increased hardening for each iteration of testing; we have witnessed sophisticated security against complex tests – showing progressive efforts against the challenges of the latest network environments while immediately and effectively addressing any previously noted vulnerabilities in prior reports
- No vulnerable ports or servers were found on MFP devices or Remote Service Platform that could leave the local network or web server at risk to attack
- IPsec spoofing attack was unsuccessful against the countermeasures in place for the Remote Service Platform
- Brute force attacks made on the Remote Service Platform/AWS Cloud were unable to compromise data or network ingress, but countermeasures are assumed to be passively blocking as they could not be verified from the attacking endpoint

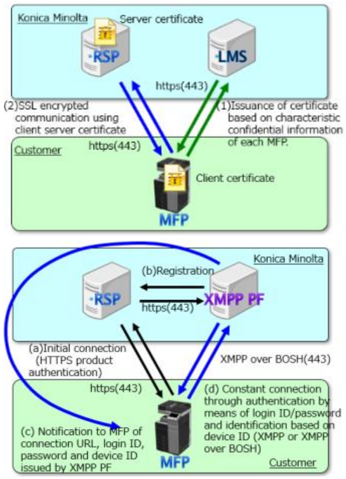
Based on our findings, Konica Minolta products and services have consistently demonstrated superior resiliency and security against real-world exploits. We proudly award Konica Minolta Remote Service Platform and managed MFDs the ***Miercom Certified Secure*** certification.

Robert Smithers
CEO, Miercom

2.0 Test Summary for Security Evaluation MFP and Remote Service Platform

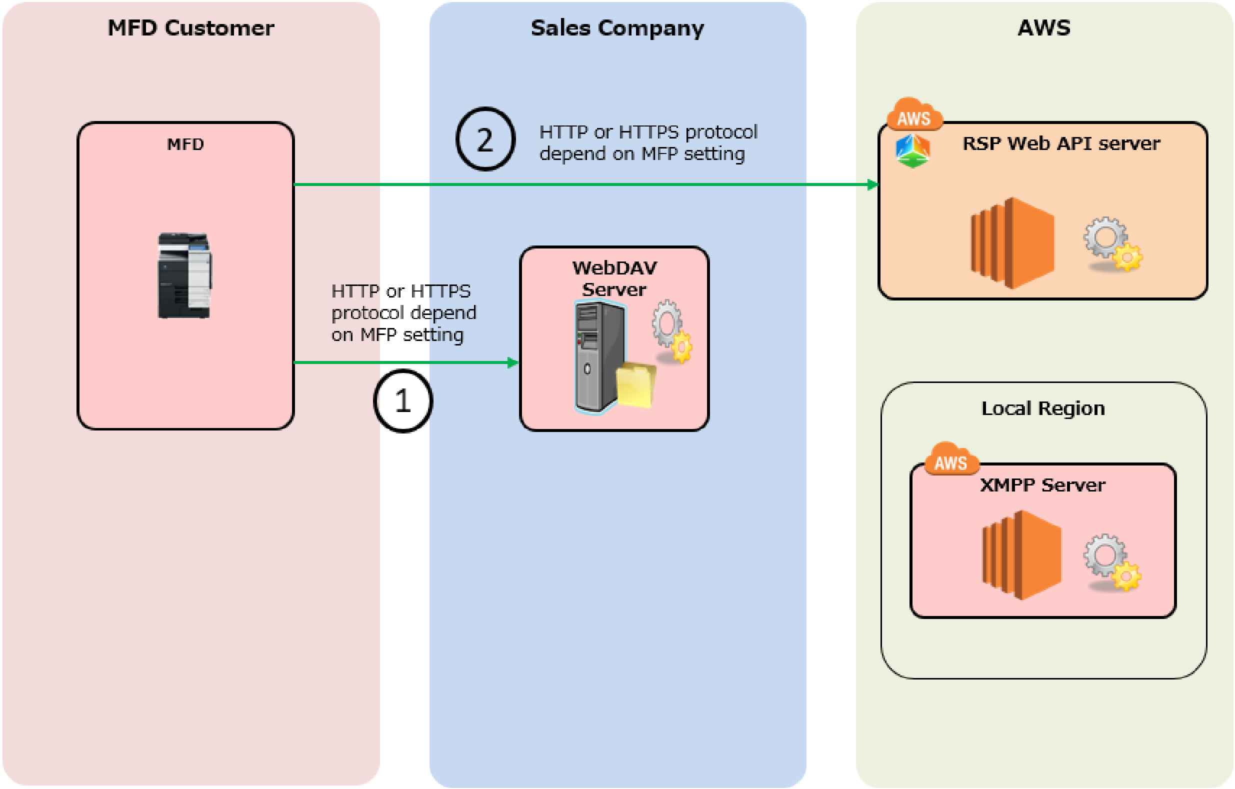
Test	Pass/Fail
Port Scan of all Cloud and Endpoint Devices	Pass
IPsec Spoofing	Pass
Miercom Proprietary Brute Force Attack	Pass
Medusa Brute Force Attack	Pass
Hydra Brute Force Attack	Pass
Cloud Management/Controller Spoofing	Pass
XMPP Exploits	Pass
MFP Driver Exploits	Pass
Miercom Proprietary Vulnerability Scans	Pass
Nikto Vulnerability Scans	Pass
Legion Vulnerability Scans	Pass
Nmap Vulnerability Scans	Pass
Privileged Areas Access of Cloud Service	Pass
SSL Extraction Keys and other Cryptographic Credentials	Pass
Web Vulnerabilities (OWASP Model)	Pass
Certificate/DNS Spoofing	Pass
DDoS Attacks	Pass
Crawljax Spider – Directory Crawler	Pass
Ajax Spider – Directory Crawler	Pass
DirBuster – Penetration Test	Pass
Zap Forced Browse Web Vulnerability	Pass

3.0 Product Overview


Konica Minolta
Server certificate
RSP
LMS
https(443)
(2)SSL encrypted communication using client server certificate
(1)Issuance of certificate based on characteristic confidential information of each MFP.
Customer
https(443)
Client certificate
MFP
Konica Minolta
(b)Registration
RSP
https(443)
XMPP PF
(a)Initial connection (HTTPS product authentication)
XMPP over BOSH(443)
https(443)
(d) Constant connection through authentication by means of login ID/password and identification based on device ID (XMPP or XMPP over BOSH)
(c) Notification to MFP of connection URL, login ID, password and device ID issued by XMPP PF
MFP
Customer

The Konica Minolta Remote Service Platform handles encrypted data communication and storage between branch and data center networks. Remote Service Platform prevents attacks on network Multifunction Printers (MFPs) using client server authentication, global IP address restrictions and other counter security measures.

Remote Service Platform Web API server communicates with License Management Servers (LMS) via HTTPS-based client and server authentication to ensure secure communication and avoid spoofing. Similarly, Remote Service Platform communicates to the XMPP server for MFP data. This two-way communication is encrypted, with limited IP addresses. The XMPP server then communicates with the MFP using an encrypted protocol.



The MFP stores setting data and log files using the WebDAV server at the business server via HTTP/HTTPS, and acknowledgment is made from the MFP to the Remote Service Platform over HTTP/HTTPS to request the download of the result. The WebDAV server grabs the file from the Amazon Cloud (AWS) to the MFP and reboots.

Secure HTTPS/SSL communications between XMPP and the MFP are carried out via BOSH over port 443. Security is implemented on both ends (XMPP and Remote Service Platform); tokens are shared between cloud services, and the MFP communicates to both to authenticate each.

This communication scheme becomes a potential attack surface for Man-in-the-Middle or brute force attacks. We tested this platform by putting our attack server in front of the AWS endpoint of the Konica Minolta services, and launching attacks against either the client or servers.

These remote operations are critical in a modern networking environment, particularly in the current pandemic climate of COVID-19, where remote upgrades and installs are preferred over on-site maintenance via USB.

Using Remote Service Platform, customers can benefit from the following seamless business services:

- **Device Firmware Upgrades:** Remote Service Platform ensures automated, scheduled upgrades for optimal performance and the latest security patches
- **System Log Acquisition/Self-Diagnosis:** In instances of MFP malfunction, intelligent data collection allows for easy self-diagnosis and remote maintenance by staying ahead of service needs to prioritize tasks that decrease downtime and cost
- **Data Backup:** With reliable data backup and data retrieval, MFP settings are saved for recall
- **Remote Panel:** Konica Minolta IT services are available for off-site troubleshooting for quick remediation that helps networks avoid downtime

4.0 How We Did It

In a lab environment, Miercom evaluated the Konica Minolta Remote Service Platform system by subjecting its individual components to vulnerability testing and analysis. Miercom used its proprietary Miercom Test Suite, Nmap and Nessus tools to carefully inspect components for security flaws. To obtain the Miercom Certified Secure accreditation, Miercom requires that no high-risk vulnerabilities be found.

The test environment consisted of a Web Distributed, Authoring and Versioning (WebDAV) server, Remote Service Platform server (AWS), two Multi-function Printers (MFPs), and multiple client devices. The AWS server was scanned and attacked within Amazon's Terms of Use restrictions, regarding Denial-of-Service (DoS) and Distributed DoS (DDoS) directed at its cloud service.

The devices connected to the cloud-based Remote Service platform communicate via HTTPS/XMPP over HTTP SSL traffic (BOSH, port 443) and multi-layer message authentication (e.g. geo-ip-fencing, message ID/sender ID matching, native IDs). We analyzed the possibility of spoofing and other vulnerabilities over these communications to determine if the cloud-based platform could be penetrated.

We tested this network using two MFPs: C360i and C458 printers connected to the Remote Service Platform via WebDAV server. The vulnerability surface consisted of impersonating either the cloud or the MFP to inject attacks. Given the nature of the platform, we also performed standard vulnerability scanning for open ports that may leave the network and endpoint devices at risk.

Test Tools

Source: Miercom

LiveAction Omnipeek is a portable network analyzer with an intuitive graphical interface for analyzing and troubleshooting enterprise networks by recording and replaying traffic snapshots via packet captures (PCAPs).

DirBuster 1.0 a java application that is designed to search for hidden pages and directories by brute forcing web and application servers.

Miercom Advanced Offensive Security Test (AOST) Suite is a collection of tools and repositories of sophisticated, legacy, and modified attacks and vulnerabilities that deep-dive into inherent and possible risks of the system or solution under test. These tools range from sponsored to open-source resources and are updated regularly to reflect the latest attack surface of the modern network.

Nmap 7.90 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.

OWASP ZAP 2.9.0 (Open Web Application Security Project) is an international non-profit organization dedicated to web application security which focuses on the top risks network administrators should look to minimize and/or mitigate. These vulnerabilities include: SQL injection, broken authentication, attacks related to sensitive data exposure and encryption, XML external entities, broken access control, security misconfiguration, cross-site scripting, insecure deserialization, inherent vulnerabilities related to system components, and insufficient logging and monitoring.

Wireshark is an open-source network protocol analyzer for monitoring and capturing network activity. Its rich feature set allows deep inspection of hundreds of protocols, live capture, offline analysis, multi-platform support, display filters and decryption.

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.

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.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.