KYOCERA Document Solutions America, Inc.

Fax Vulnerability White Paper V. 1.5

(Fax Architecture A)

Business Services Support

May 2020

Version 1.5

History of Revision(s)

Date	Version	Description	Author
08/2018	1.20	English Version	Mark DeSarno
03/2019	1.30	English Version	Mark DeSarno
10/2019	1.40	English Version	Mark DeSarno
05/2020	1.5	English Version	Mark DeSarno

CONTENTS

1 Preface

1.1 Purpose

This document is intended for KYOCERA customers to better understand how KYOCERA Multi-Function Products, with the fax option attached, are designed to guard against outside intrusion through the analog phone line connected to our devices with fax systems in the field. The following KYOCERA Technical White Paper information is considered to be a security-based technical document.

- **Fax Line Separation from Main MFP Systems and Clients Internal Network**
- **Memory Usage, Access and ITU Standards and Compliance**

KYOCERA Security Technical White Papers, including this document, describe KYOCERA security measures and features against various security threats to KYOCERA products.

This document focuses on security measures against unauthorized access to KYOCERA products or to user environments connected to its products via a telephone line, which is one of the interfaces used by KYOCERA products with the fax option.

1.2 Scope

The focus of this document is on security measures for KYOCERA products listed.

1.3 Definitions, Initials, and Abbreviations that are utilized within this document

MFP: Multifunction Product (Devices that provide Print, Copy, Scan and Fax features)

LAN: Local Area Network (A network inside your location for computers and other devices to communicate)

FTP: File Transfer Protocol (Used to transfer files between computers on a network)

SFTP: Secure File Transfer Protocol (Secure transfer of files between computers on a network)

SMB: Server Message Block (A protocol for sharing files, printers, and communications between computers)

RAM: Random Access Memory (A random-access memory device allows data items to be read or written in almost the same amount of time, which can be accessed randomly)

1.4 Summary

This document describes the KYOCERA product environment, potential threats, assets to protect, features summary, and KYOCERA security measures.

2 KYOCERA Products Environment

2.1 Growing Interest in Information Security

The technologies of communication and information infrastructure are changing rapidly. Along with benefits, the changes bring threats to information assets. Information leaks and falsification caused by network attacks from the outside and information leaks from the inside have been reported by IT teams worldwide. The news media often reports cases of personal and confidential information leaks.

KYOCERA MFPs are embedded with an operating system, storage, and communication capabilities. These are used in the information system of the users' organization and network environment. KYOCERA MFPs handle confidential and protected information to prevent a network attack, information flow, leakage, and falsification.

In addition to servers, network devices, and computers, MFPs under the users' organization network must have information security in place.

2.2 KYOCERA Product Development Approach

KYOCERA believes that safeguarding the users' information is an important mission of the company. Protecting and improving the users' experience is a top priority. To counteract embedded vulnerabilities, KYOCERA has implemented security measures that help fight against any threat. Products are designed to maintain a high level of information security.

3 Potential risk presented to Multi-Function Product (MFPs) Fax Platform

3.1 Threat from an analog phone Line (Unauthorized Access to the Network)

An MFP has numerous interfaces that provide convenient features and a network interface for printing, scanning, and sending. In addition, an MFP (with Fax) has an analog phone line interface for connecting to an analog phone line for transmitting and sending faxes.

Threats can occur if the interfaces are compromised. A possible risk is that an outside person could access an MFP through an analog phone line and illegally access an organization's network.

MFPs are generally located in offices where the network is protected from the Internet by a firewall. Illegal access to an organization's network environment is difficult to achieve from the outside. However, because a telephone line is an interface directly connected to the outside, a third-party person can gain access to the MFP. This creates a potential threat of unauthorized access to the LAN through the MFP.

3.2 KYOCERA Products System Configuration

The KYOCERA products system configuration is illustrated in Figure 1.

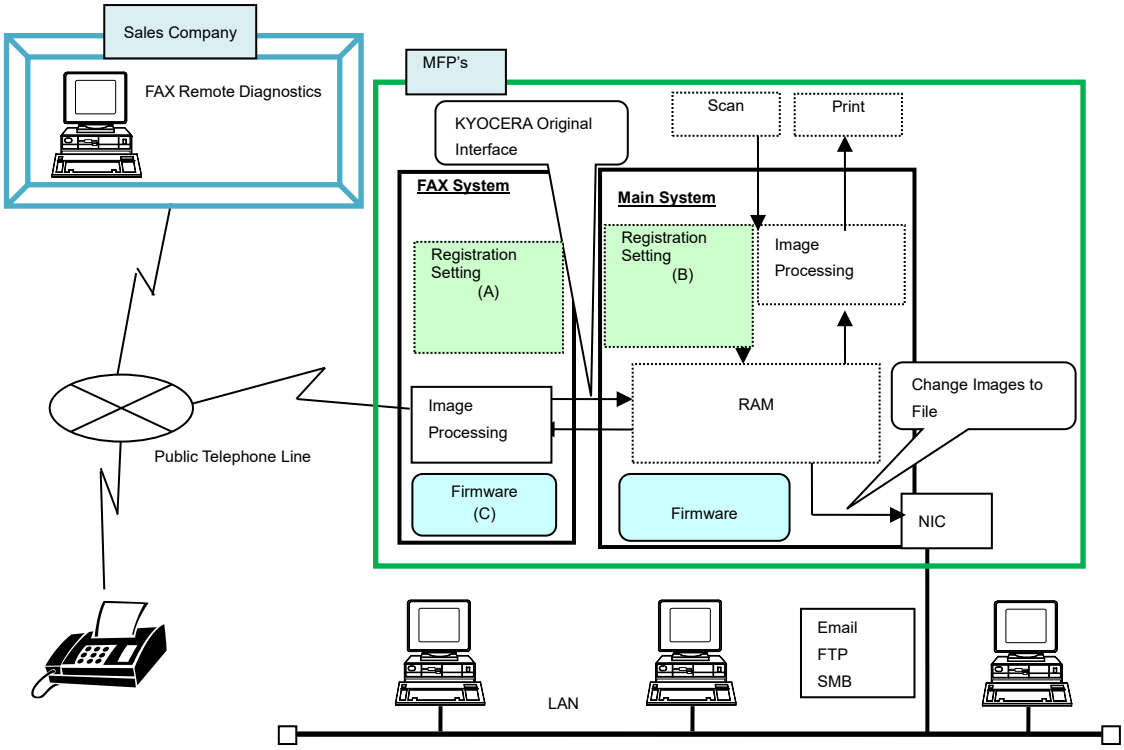

Figure 1 KYOCERA Products System Configuration

In the Figure 1 configuration, the Main System and FAX System exist independently. The Main System controls the Copy and Print features and part of the FAX feature. The FAX System controls FAX transmittal and reception. Firmware in each system manages image processing and the registration setting. The FAX feature requires both Main System and FAX System.

4 KYOCERA Product Security Features

KYOCERA products provide the following protection features against the threat of unauthorized access from a public telephone network (line):

4.1 Countermeasures against accessing the Internal Network from a Analog phone Line

1) Accessing the FAX System from a telephone line

- The FAX System communicates with other devices using the G3 protocol as defined for FAX transmission by the ITU-T. FAX data is received as Black and White (B&W) image data only.

- KYOCERA MFPs only accept facsimile protocols from the phone line connection. (Any communication using other protocols will be rejected.)

2) Accessing the Main System from the FAX System:

- The FAX System forwards the received ITU-T B&W image data, via a telephone line to the Main System RAM.
- The Main System handles the RAM data as bitmap B&W image data and prints it as hardcopy or converts it to the user's selected image data.

3) Accessing the Network from the Main System

- When using the FAX memory forward feature, the B&W image data forwarded to the Main System RAM is converted to a selected image file format set by an administrator (PDF,TIFF, XPS) and sent to a computer folder or FTP Server specified on the network. It also can be sent as an e-mail attachment for secure delivery to the intended recipient, limiting who can view the documents to help your office meet a certain level of compliance when required.
- When the RAM data is converted into one of the selected choices above, it is compressed as B&W image data. Wherever the data is sent, via the network, it is handled as image files.

4) Accessing the network from an analog phone line

- As the configuration shows, the telephone line and the network have separate architecture, so there is no direct data path between interfaces.

With the configuration described in items 1-4, unauthorized access to the network from a telephone line is not possible.

4.2 FAX Remote Diagnostics Transmission

KYOCERA Fax Remote Diagnostic transmission uses software to create diagnostic reports of registered information and data settings and edit individual transmission settings, executed by utilizing a format of a KYOCERA confidential receive facsimile image.

When referring or changing the registration setting data, the following security measures are taken against security risks:

- KYOCERA's confidential FAX transmission sequence is followed.
- The data format is a special format used in Universal Remote Diagnostic System (URDS).
- The utility used in URDS is provided to sales companies only, not to general users.

KYOCERA Products System Configuration contains three types of received and transmitted data: FAX System Registration, Setting of Data, and FAX System Firmware.

The Command from a PC consists of a KYOCERA original transmission sequence, and the command contains only protocols that update the Fax system firmware. It is impossible to change any other firmware inside the MFP, and it is also impossible to send data to any internal network-connected components.

Communication between the Fax system and all other components within the device is limited to the transferring of bitmap image data.

KYOCERA Products System Configuration

1) Changing data using a FAX Remote Diagnostics Transmission

   - Secure URDS commands sent from the FAX Remote Diagnostics Software installed on a computer can change the registration setting data of the FAX System and the registration setting data (Address book only).
   - Secure URDS commands sent from a computer consists of a KYOCERA original transmission sequence and contains only the protocol that changes the FAX System firmware. It is not possible to change any other firmware within the MFP. It is also not possible to send data into the internal network-connected portion of the MFP.

2) Viewing data using a FAX Remote Diagnostics Transmission

   - A command sent from the FAX Remote Diagnostics Software installed on a computer can retrieve the registration setting from the FAX System and the registration setting data (address book and print counter information) through a telephone line.
   - A command sent from a computer consisting of the KYOCERA original transmission sequence uses a protocol that can only retrieve the previously-mentioned data. It is not possible to view the internal network data via a telephone line.

5. Additional security and safety features KYOCERA offers:

- Print and hold received Faxes for secure view only
- Repeat entry of fax number option to ensure sending to the correct location
- Destination confirmation when one touch dialing is selected to ensure correct location

6. Supported KYOCERA and Copystar Models

B&W	Color
TASKalfa/CS 8002i	TASKalfa/CS 8052ci
TASKalfa/CS 8001i	TASKalfa/CS 7551ci
TASKalfa/CS 7002i	TASKalfa/CS 7052ci
TASKalfa/CS 6501i	TASKalfa/CS 6551ci
TASKalfa/CS 6002i	TASKalfa/CS 6052ci
TASKalfa/CS 5501i	TASKalfa/CS 5551ci
TASKalfa/CS 5002i	TASKalfa/CS 5052ci
TASKalfa/CS 4501i	TASKalfa/CS 4551ci
TASKalfa/CS 4002i	TASKalfa/CS 4052ci
TASKalfa/CS 3511i	TASKalfa/CS 3552ci
TASKalfa/CS 3501i	TASKalfa/CS 3551ci
TASKalfa/CS 3011i	TASKalfa/CS 3252ci
TASKalfa/CS 3010i	TASKalfa/CS 3051ci
FS-6530MFP	TASKalfa/CS 2552ci
FS-6525MFP	TASKalfa/CS 2551ci
FS-3640MFP	TASKalfa/CS 205c
FS-3140MFP+	TASKalfa/CS 406ci
FS-1135MFP	TASKalfa/CS 356ci
ECOSYSM3650idn	TASKalfa/CS 306ci
ECOSYS M3550idn	FS-C2626MFP
ECOSYS M3540idn	FS-C2126MFP+
ECOSYS M2535dn	FS-C8525MFP
ECOSYS M4132idn	FS-C8520MFP
ECOSYS M4125idn	ECOSYS M6535cidn
TASKalfa/CS 9002i	ECOSYS M6526cidn
ECOSYS M3660idn	ECOSYS M6530cidn
ECOSYS M3655idn	ECOSYS M6526cdn
ECOSYS M3145idn	ECOSYS M8130cidn
ECOSYS M3645idn	ECOSYS M8124cidn
TASKalfa/CS 4012i	TASKalfa/CS 307ci
TASKalfa/CS 3212i	ECOSYS M6235cidn
TASKalfa/CS 4003i	ECOSYS M6630cidn
TASKalfa/CS 5003i	ECOSYS M6635cidn
TASKalfa/CS 6003i	TASKalfa/CS 2553ci

B&W	Color
TASKalfa/CS 7003i	TASKalfa/CS 3253ci
TASKalfa/CS 8003i	TASKalfa/CS 3553ci
TASKalfa/CS 9003i	TASKalfa/CS 4053ci
	TASKalfa/CS 5053ci
	TASKalfa/CS 6053ci
	TASKalfa/CS 7353ci
	TASKalfa/CS 8353ci
	TASKalfa/CS 408ci
	TASKalfa/CS 358ci
	TASKalfa/CS 308ci
	TASKalfa/CS 508ci

For additional support or information please contact your Authorized Kyocera or Copystar Sales Representative

Specifications and design are subject to change without notice.
KYOCERA is a trademarks of Kyocera Corporation in the United States and/or other countries..Other trade names in this White Paper are the trademarks of their respective owners.

PLEASE NOTE: This document is provided for information purposes only. KYOCERA does not warrant or guarantee that the customer's Kyocera MFPs or printers have been equipped or have the proper security or specifications for their needs or requirements. Supported security functions or specifications vary and may require optional equipment. For more information, please refer to the catalogs or user manuals for the detailed features of each product