MULTIFUNCTION DEVICE AND NETWORK PRINTERS SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 14

25 October 2019

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Multifunctional Devices (MFDs) and Network Printers Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to MFDs, network-attached printers, and digital sender technologies. Thus, directly connected printing devices such as USB printers are out of scope. Although MFDs often include fax services, network fax servers are outside the scope of this document. The MFD checklist is meant for use in conjunction with the Network Infrastructure and appropriate operating system (OS) STIGs.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configurations settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system’s particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device-hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. CONCEPTS AND TERMINOLOGY CONVENTIONS

2.1 Introduction

The purpose of this section is to discuss the general principles involved in security network-attached MFDs, digital senders, and network printers. MFDs provide printing, copying, faxing, and scanning services from a single network-accessible device. This consolidation of services into one device saves both space and money. Similar to computers, MFDs and many network printers include an operating system (usually embedded) and network connectivity. These devices also can use similar network protocols, such as File Transfer Protocol (FTP), telnet, Hyper Text Transport Protocol Secure (HTTPS), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). MFDs may also have a connection to a phone line for fax functionality. As more functionality has been added to these devices, the security vulnerabilities and risk to organizational data are becoming similar to those of other network clients.

The following are a minimum set of features that are required on each device to support security policy and risk mitigation. Devices must have the capability to:

- Update the firmware.
- Disable unneeded services, protocols, and features.
- Restrict access to the device based on IP address.
- Allow setting and changing of the authentication information (e.g., passwords and community strings) for all management services.
- Prevent unauthorized physical access to the hard drive using either a locking mechanism or other physical access control measure.
- Implement authenticated access to management controls, allowing access to authorized administrators based on privilege assignments.
- Enable and configure audit logging (Syslog capability preferred).

2.2 Management Services

As the name implies, management services are the services used by the device to allow administrative access to configure and monitor the device. FTP, SSH, HTTP, HTTPS, SMTP, BOOTP, DHCP, and SNMP are the most common services. Like their server counterparts, there is a potential for unauthorized access or compromise through these services.

In most cases, FTP and SSH are not needed except for the occasional firmware upgrade. HTTP and HTTPS are used to remotely manage the device through an embedded web server. DHCP is disabled because the device will have a dedicated IP. SMTP is used to inform system administrators of critical errors (low toner, paper jams, and low paper). SNMP is used for network monitoring. HTTPS is used instead of HTTP and SNMPv3 is preferred over earlier versions.

The default passwords or community strings on these services are replaced with a complex password, and all unneeded services are disabled. Unless using HTTPS or SNMPv3, services needed for firmware upgrades or device configurations are enabled only when needed. All other management services (e.g., Dynamic Host Configuration Protocol [DHCP], SMTP, Bootstrap Protocol [BOOTP], etc.) are disabled at all other times.

It is recommended that all MFDs and printers be placed on a dedicated network segment or virtual local area network (VLAN) with a discretionary access list to limit access to IPs of the print spoolers and System Administrators. With this configuration, users will not be able to directly access the devices but rely on print spoolers and the additional security they provide.

If a device does not allow a compliant configuration (i.e., does not support disabling services, resetting passwords, updating firmware, passwords, and configuration, is lost after shutdown (older printers), IP restrictions, or any other requirement related to device configuration, the vulnerability will be mitigated by at least one of the following:

- Replace the print server with another internal or external print server that allows a compliant configuration.
- Place the device behind a switch, router or firewall allowing a discretionary access list to block all traffic to the device except the traffic coming from the print spooler and System Administrators IP.

2.3 Network Printing Services

2.3.1 Network Protocols

Printers offer many options for network and printing protocols, depending on the needs of the network environment. However, the use of TCP/IP is required in DoD. MFDs and network printers must be configured using a static IP address. All unnecessary or unauthorized protocols, functions, and services must be disabled to prevent exploitation. Since some vendor firmware upgrades or maintenance actions may re-enable these services, it may be necessary to periodically verify these services have remained disabled.

Most modern MFDs and printers are capable of employing a number of print services to include: Port 9100, line printer daemon (LPD), Internet Printing Protocol (IPP), and FTP. In most cases, only Port 9100 or LPD is necessary. For Windows-based systems that use a print spooler, use Port 9100 only. UNIX, Linux, and Mainframe systems use LPD (port 515). Where both Windows and non-Windows clients need services from the same device, both Port 9100 and LPD may be enabled.

2.4 Fax Services

The MFD often includes traditional fax services where the fax is delivered and printed or held at the device itself. However, fax servers are not within the scope of the MFD guidance at this

time. Fax servers are devices or applications that enable users to send, receive, and manage documents directly from desktop, email, and other business applications.

2.5 Physical Security

MFDs and printers share many of the same security concerns as network servers. However, unlike network servers, printers are installed in the general work spaces rather than in a secured server room. Lowering the risk of tampering and unauthorized physical access is imperative. If the device has a hard disk, the device must employ a physical or logical method of security to protect the hard drive from unauthorized access. Access to the device's configuration and management functions from the console must be secured against access by non-privileged or unauthorized individuals. For repairs to the device by a vendor, the controls may be relaxed then put in place after repair. Print, scan, copy, and fax jobs must be secured against unauthorized access and deleted when no longer needed. Securing network printing devices will minimize the loss of confidential data recovered in the event the hard drive is stolen or the printer is otherwise compromised.

2.6 Wireless Direct Printing

Direct wireless printing features, such as Apple AirPrint and HP Wi-Fi Direct, allow mobile device users the ability to print directly to a MFD or printer. Wireless direct printing bypasses the print spooler, which prevents authentication of the user and logging of print jobs. Wireless direct printing features must be disabled on MFDs and printers.