MICROSOFT (MS) EXCHANGE 2013 CLIENT ACCESS SERVER (CAS) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

25 July 2016

Developed by Microsoft and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Exchange 2013 Client Access Server Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. This document is meant for use in conjunction with the Windows Operating System (OS) STIG and any appropriate STIG(s) applicable to the system.

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 provides 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 configuration 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 percent 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 the 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. REFERENCE DOCUMENTS

The following table enumerates the documents and resources referenced:

Table 2-1: Reference Documentation

Date	Document Description	Source
February 2014	Microsoft Exchange Server 2013	https://technet.microsoft.com/en-us/library/bb124558(v=exchg.150).aspx
Current Version	Windows Server 2008 R2 STIG	http://iase.disa.mil/stigs/os/Pages/index.aspx
Current Version	Windows Server 2012 STIG	http://iase.disa.mil/stigs/os/Pages/index.aspx
April 2013	SP 800-53 Security and Privacy Controls in the Federal Information Systems and Organizations	http://csrc.nist.gov/publications/PubsSPs.html
February 2006	SP 800-18 Guide for Developing Security Plans for Federal Information Systems	http://csrc.nist.gov/publications/PubsSPs.html
February 2007	SP 800-45 Guidelines on Electronic Mail Security	http://csrc.nist.gov/publications/PubsSPs.html
April 2015	Network ports for clients and mail flow in Exchange 2013	https://technet.microsoft.com/en-us/library/bb331973(v=exchg.150).aspx

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Operational View

Email systems are composed of multiple products and services working together to enable transport and delivery of messages to users. This overview gives background and information specific to MS Exchange 2013 Client Access Server.

MS Exchange 2013 introduced a number of architectural and fundamental changes compared to Exchange 2010. In Exchange 2013, the Client Access and Mailbox roles host the services previously handled by the Hub Transport, Client Access, Mailbox, and Unified Messaging roles. The Hub Transport role from 2010 is now split between the Client Access Server and Mailbox Server roles. The Unified Messaging role from 2010 is now combined into both Mailbox and CAS roles.

The CAS role is the initial point of contact for end users seeking email access. Applications such as Outlook Web App (OWA), Outlook Anywhere (OA), and Outlook, as well as mobile technologies servers and public folders requests, are processed through the CAS.

Commercial Mobile Devices (CMD) communicate with the CAS through protocols such as Exchange ActiveSync (EAS) to provide email services. Current CMD policy (DoD CIO memo dated 06 Apr 2011) requires mobile devices to communicate using Mobile Email Management (MEM) servers that act as intermediaries between the email server and the CMDs. The CAS also depends on MS IIS web services, which must be reviewed prior to performing the CAS review.

For an overview of all the MS Exchange Server 2013 products and services, reference the MS Exchange Server 2013 Server STIG Overview document at the following URL:

http://iase.disa.mil/stigs/app-security/app- servers/Pages/index.aspx.

The MS Exchange Server 2013 STIG Overview also includes security review considerations to prepare for periodic assessments.