McAfee Anti-Virus

Technology Overview

Version 4, Release 10

24 January 2014

Developed by DISA for the DoD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

This Desktop Anti-Virus Technology Overview, along with the associated Desktop Anti-Virus STIG, provides the technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) applications.

The nearly universal presence of systems on the desktops of all levels of staff provides tremendous opportunities for office automation, communication, data sharing, and collaboration. Unfortunately, this presence also brings about dependence and vulnerabilities. Malicious and mischievous forces have attempted to take advantage of the vulnerabilities and dependencies to disrupt the work processes of the Government. Compounding this problem is the fact that the vendors of software applications have not expended sufficient effort to provide strong security in their applications. Where applications do offer security options, the default settings typically do not provide a strong security posture.

This document provides general guidance on some of the commonly found desktop applications in the most commonly found desktop operating system environments. Web browsers and e-mail clients were given priority, because they are most common. Antivirus products, because of their strategic importance in preventing problems, were also a priority. Other applications were added as specific requirements were identified.

1.1 Background

Even though this document addresses the security of COTS applications rather than an operating system, it is not possible to completely separate the security issues. Security is an attribute of the whole as well as of each of the parts. In accordance with this philosophy, the same policies and guidance that apply clearly to operating systems are also applicable to applications.

The applications addressed in this document utilize mobile code and Public Key Infrastructure (PKI) technologies to enable some of their features. The requirements described in this document are designed to implement the applicable Department of Defense (DoD) polices for those technologies. These policies are described in the *Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems* (later referred to as the DoD Mobile Code Policy) and the *Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling* documents, as referenced in *Appendix C, Related Publications*.

1.2 Authority

DoD Directive (DoDD) 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoDD 8500.1. "Although the use of the principles and guidelines in this STIG provide an environment that contributes to the security requirements of DoD systems operating at Mission Assurance

Category (MAC) codes I through III, all DoDI 8500.2 IA controls need to be applied to all systems and architectures."

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Officer (IAO) will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

It should be noted that Field Security Operations (FSO) support for the STIGs, and Tools is only available to DoD customers.

1.3 Scope

The requirements and recommendations set forth in this document will assist IAOs and Information Assurance Managers (IAMs) in protecting desktop applications in DoD locations hereafter referred to as sites. The responsible Configuration Control Board (CCB) will approve revisions to site systems that could have a security impact. Therefore, before implementing desktop application security measures, the IAO will submit a change notice to the CCB for review and approval.

Although there are a few different operating system platforms for desktop environments, this document addresses applications running on Microsoft Windows platforms. This document does not include specific guidance for UNIX or Linux or Apple desktop environments at this time.

The security requirements detailed in this document apply to applications installed on Microsoft Windows Server platforms as well as Microsoft Windows Workstation platforms. On server platforms, the security configuration parameters will be set to at least as restrictive values as those listed in this document.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**". The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written.

For each italicized policy bullet, the text will be preceded by parentheses containing the STIG Identifier (STIGID), which corresponds to an item on the STIG and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*)." If the item presently does not have an STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "*[N/A: CAT III]*"). Throughout the document, accountability is

directed to the IAO to "ensure" a task is carried out or monitored. These tasks may be carried out by the IAO or delegated to someone else as a responsibility or duty.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. All reasonable attempts to meet this criterion will be made.

1.5 Vulnerability Severity Code Definitions

Table 1-1. Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow super user access, or bypass a firewall. This includes a vulnerability that would allow execution of Category 1X mobile code and unsigned Category 1A mobile code.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder. This includes inappropriate execution of Category II mobile code.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVM notifications are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert.

1.7 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as scripts, and other related security information.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

This page is intentionally left blank.

2. GENERAL INFORMATION

This document, and associated STIG, has set forth requirements based upon having a secured Windows environment as described in various other documents. These documents include various National Security Agency (NSA) guides (found at http://www.nsa.gov/snac/) and Windows STIG's available from the IASE web site (http://iase.disa.mil/). Failure to follow these requirements can significantly diminish the value of many of the specifications in this document.

Security controls that are managed through the underlying operating system platform directly affect the strength of the security that surrounds desktop applications. This section highlights some measures that are taken to increase that strength.

This section of the document provides the following categories of information:

- Considerations for the terminology and content of this document
- Information relevant to general desktop application security that is not specific to an individual product
- Limited guidance on individual products or categories of products that are not covered in subsequent chapters

2.1 Terminology Conventions

Current desktop applications present a graphical user interface (GUI) for their use and parameter customization. Most of the parameter settings specified in this document can be examined and changed through the application's GUI, subject to Windows policy settings. The following terms are used in describing how to view or configure the settings:

- Dialog – An application dialog is a window presented by the application.
- Menu – An application menu consists of a textual list of actions, commands, or (sometimes) options that can be selected.
- Enable – The term enable is used to describe the selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies "enable", the associated option button display would indicate that the option is selected.
- Disable – The term disable is used to describe the de-selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies "disable", the associated option button display would indicate that the option is de-selected.

2.2 Methods of Review

2.2.1 Automated Review

To conduct an automated self-assessment or SRR for the Desktop Anti-virus STIG requirements, DISA FSO develops and maintains the DISA Gold Disk. DISA FSO produces this tool to aid in the security assessment process as well as the remediation process of Microsoft Windows systems. The Gold Disk distribution contains a fully documented user's guide, the *Windows Gold Disk User's Guide for Version 2*, to assist system administrators (SAs) and reviewers in the use of the Gold Disk. The reviewer uses the output of the Gold Disk to analyze and document potential security vulnerabilities on the reviewed system. This output can then be used as input to the VMS.

Use the most recent version of the Gold Disk available to conduct the assessment. The Gold Disk is available from http://iase.disa.mil/stigs/SRR/index.html and https://patches.csd.disa.mil/Default.aspx.

2.2.2 Manual Review

To conduct a manual review of compliance with the Anti-Virus STIG requirements, it is necessary to use some tools that are provided with the Windows operating system. Some of these tools are as follows:

Windows Explorer
Windows "Edit File Type" facility – accessed through the Windows Explorer
Windows Registry Editor – regedit.exe or regedt32.exe
Windows Search – accessed via the Windows Start Menu
Microsoft Management Console (MMC)
Microsoft Security Configuration and Analysis snap-in (used with the MMC)

Additionally, many of the settings required in this document must be set using dialogs provided by the applicable application. Such dialogs would include the use of pull-down menus, tabs, and GUI windows.

Instructions for the manual remediation of vulnerabilities to include adding, deleting, and modifying settings can be found in the "Fix" information provided in the VMS vulnerability description.

2.3 Other Considerations

It must be noted that the guidelines specified should be evaluated in a local, representative test environment before implementation within large user populations. The extensive variety of environments makes it impossible to test these guidelines for all potential software configurations. For some environments, failure to test before implementation may lead to a loss of required functionality.

2.4 Open Source/Freeware

DoD has clarified policy on the use of open source software (OSS) to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. DoD no longer requires that operating system software be obtained through a valid vendor channel and have a formal support path, if the source code for the operating system is publicly available for review.

From the DoD Chief Information Officer (CIO) memo, "Open Source Software (OSS) in Department of Defense (DoD), 28 May 2003":

> "DoD Components acquiring, using or developing OSS must ensure that the OSS complies with the same DoD policies that govern Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) software. This includes, but is not limited to, the requirements that all information assurance (IA) or IA-enabled IT hardware, firmware and software components or products incorporated into DoD information systems whether acquired of originated within DoD:
>
> Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and be configured in accordance with DoD approved security and configuration guidelines.

OSS takes several forms and may be acceptable or unacceptable depending on the form:

1. A utility that has publicly available source code is acceptable.
2. A commercial product that incorporates OSS is acceptable because the commercial vendor provides a warranty.
3. Vendor supported OSS is acceptable.
4. A utility that comes compiled and has no warranty is not acceptable.

The DoDD 8500.1 states "Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA."

APPENDIX A: General Anti-Virus Guidance

A.1. Anti-virus Information

Next to properly configured operating system security controls, effective antivirus software is the most critical tool in securing desktop application systems. The value of an up-to-date software with current virus definition files cannot be underestimated. Malicious programs that result in a denial of service (DoS) or corruption of data can be thwarted with antivirus programs that look for signatures of known viruses and take preventative action.

The use of products by DoD organizations, other than those available on the JTF-GNO web site, is discouraged. DoD has special licensing agreements with both McAfee and Symantec.

It must be noted that the guidelines in this section have been written to apply to clients whether on a server or workstation. Using these guidelines for mail servers do not provide appropriate or adequate protection for servers running complex applications (such as Microsoft Exchange or Lotus Notes). Additional antivirus measures need to be taken on mail servers.

The JTF-GNO makes several antivirus tools available for download from its web site at https://www.jtfgno.mil/antivirus/antivirus_index.htm. These products are also available for download on the DoD Patch Repository at https://patches.csd.disa.mil.

The following sub-sections provide general guidance that applies to all antivirus software.

It is recommended that signatures files be updated daily.

A.1.1 General Guidance for Antivirus Software

This section details general guidance for the configurations of antivirus products.

Scans at boot time (or daily) are recommended when this would not cause a significant impact to operations.

The following file types are particularly vulnerable as the host for a virus. These file types must be included in the antivirus scan:

- Executable, service and driver files (i.e., files suffixed with .bat, .bin, .com, .dll, .exe, .sys, etc.)
- Application data files that could contain a form of mobile code (i.e., files suffixed with .doc, .dot, .rtf, .xls, .xlt, .hta, scrap objects, .wsh, etc.)

.

In the event that a virus is found, the user must be notified. This allows the user to take any additional action to reduce damage and halt propagation of the virus. The user should also exercise the appropriate computer security incident reporting requirements as defined by the site.

A.1.2 Software Maintenance

Maintaining the security of web browsers requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch to overcome security vulnerabilities.

This page is intentionally left blank.

APPENDIX B: List of Acronyms

AIS	Automated Information System
C&A	Certification and Accreditation
CA	Certificate Authority
CBC	Cipher Block Chaining
CCB	Configuration Control Board
CCK	Client Customization Kit
CDO	Collaboration Data Objects
CD-R	Compact Disk-Recordable
CD-RW	Compact Disk-Rewritable
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
COTS	Commercial-Off-The-Shelf
CVE	Common Vulnerabilities and Exposures
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center – Detachment
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DMS	Defense Message System
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	DoD Instruction
DoS	Denial-of-Service
DSN	Defense Switched Network
EAL	Evaluated Assurance Level
ECA	External Certificate Authority
FSO	Field Security Operations
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol with SSL
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
ICSA	International Computer Security Association
IE	Internet Explorer
IEAK	Internet Explorer Administration Kit
IEC	International Electro-technical Commission
IECA	Interim External Certificate Authority

IIS	Internet Information Services
IM	Instant Messaging
IMAP4	Internet Messaging Access Protocol 4
INFOCON	Information Operations Condition
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
JTF-GNO	Joint Task Force - Global Network Operations
LRA	Local Registration Authority
MAC	Message Authentication Code
MAC	Mission Assurance Category
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
MMC	Microsoft Management Console
MSDE	Microsoft SQL Server Desktop Engine
NIAP	National Information Assurance Partnership
NIPRNet	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
NSO	Network Security Officer
OLE	Object Linking and Embedding
OSS	Open Source Software
PCT	Private Communication Technology
PDA	Personal Digital Assistant
PDF	Portable Document Format
PKE	Public Key Enabling
PKI	Public Key Infrastructure
POP3	Post Office Protocol 3
RC2	Rivest's Cipher 2
RC4	Rivest's Cipher 4
RNOSC	Regional Network Operations and Security Center
RTF	Rich Text Format
SA	System Administrator
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SMAPI	Simple Messaging Application Programming Interface
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SR	Service Release
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
SSL	Secure Sockets Layer

SSO	Systems Support Office
STIG	Security Technical Implementation Guide
STIGID	STIG Identifier
TA	Trusted Agent
TASO	Terminal Area Security Officer
TLS	Transport Layer Security
UNC	Universal Naming Convention
URL	Uniform Resource Locator
VBA	Visual Basic for Applications
VM	Virtual Machine
VMS	Vulnerability Management System
WFP	Windows File Protection
WSH	Windows Scripting Host
XML	Extensible Markup Language

This page is intentionally left blank.

APPENDIX C: Related Publications

Government Publications

Department of Defense, DoD Directive (DoDD) 8552.01, "Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," 23 Oct 2006.

Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling", 24 May 2011.

Department of Defense, DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," October 24, 2002.

Department of Defense, DoD Instruction (DoDI) 8500.2, "Information Assurance (IA)," February 6, 2003.

Department of Defense, "X.509 Certificate Policy for the United States Department of Defense," Version 5.2, 13 November 2000.

Defense Information Systems Agency, "Secure Remote Computing Security Technical Implementation Guide", Current Version.

Executive Office of the President, Office of Management and Budget Memorandum, "Protection of Sensitive Agency Information", 23 June 2006.

National Security Agency (NSA), "E-mail Security in the Wake of Recent Malicious Code Incidents," Version 2.6, 29 January 2002.

National Security Agency (NSA), "Microsoft Office 2000 Executable Content Security Risks and Countermeasures," 8 February 2002.

National Security Agency (NSA), "Microsoft Office XP/2003 Executable Content Security Risks and Countermeasures," 10 February 2005.

Government Web Sites

http://www.disa.mil/ Defense Information Systems Agency
https://datahouse.disa.mil/ Defense Information Systems Agency Datahouse
http://iase.disa.mil/ (NIPRNet)
Defense Information Systems Agency Information Assurance Support Environment
https://www.jtfgno.mil http://www.cert.mil/ (NIPRNet) JTF-GNO NetDefense
https://patches.csd.disa.mil DoD Patch Repository
http://dodpki.c3pki.chamb.disa.mil/ or http://dodpki.c3pki.den.disa.mil/
Department of Defense Class 3 Public Key Infrastructure (PKI) Home Page
http://www.c3i.osd.mil/org/sio/ia/pki.html
Department of Defense Public Key Infrastructure Program Management Office(DoD PKI PMO)
http://www.nsa.gov/isso/index.html
National Security Agency Information Assurance Directorate (NSA IAD)

Commercial and Other Non-government Sites

http://www.icsalabs.com/ International Computer Security Association (ICSA) Labs
http://www.mozilla.org FireFox Information
http://www.mcafee.com/support/ McAfee Support
http://www.microsoft.com/download/en/default.aspx Microsoft Download Center
http://windows.microsoft.com/en-US/internet-explorer/products/ie/home
Microsoft IE Product Downloads
http://technet.microsoft.com/en-us/security Microsoft TechNet Security
http://www.symantec.com/techsupp/ Symantec Service & Support
http://www.wildlist.org/ The WildList Organization