MCAFEE VIRUSSCAN ENTERPRISE FOR LINUX (VSEL) 1.9x/2.0x SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

24 April 2020

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 McAfee VirusScan Enterprise for Linux1.9x/2.0x Security Technical Implementation Guidance (STIG) document provides the technical security policies, requirements, and implementation details for applying security concepts to a Commercial-Off-The-Shelf (COTS) application.

Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Malware has become the most significant external threat to most systems, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. Spyware's intention is to violate a user's privacy and has become a major concern to organizations. Although privacy violating malware has been in use for many years, it has become much more widespread recently, with spyware invading many systems to monitor personal activities and conduct financial fraud. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing, which is using deceptive computer-based means to trick individuals into disclosing sensitive information. Another common form is virus hoaxes, which are false warnings of new malware threats.

These requirements address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools, such as backdoors and root kits.

There are two individual STIG packages available for the McAfee VirusScan Enterprise for Linux 1.9x/2.0x:

- McAfee VirusScan for Linux (VSEL) 1.9x/2.0x Local Client
- McAfee VirusScan for Linux (VSEL) 1.9x/2.0x Managed Client

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 Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.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. ASSESSMENT CONSIDERATIONS

This document, and associated STIGs, has set forth requirements based on having a secured Linux environment as described in various other documents. These documents include the NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-83, Guide to Malware Incident Prevention and Handling, available from National Institute of Standards and Technology (http://www.nist.gov), and the Linux Operating System STIGs, available from the IASE website (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 STIG will be updated quarterly, as needed. The audience of this STIG should be aware of the importance of keeping current with the Task Orders, Op Orders, and Fragmentation Orders issued by USCYBERCOM.

In the event a directive issued by USCYBERCOM results in a setting to be more restrictive than this STIG, the USCYBERCOM directive will take precedence over the STIG setting.

In the event a directive issued by USCYBERCOM results in a setting to be more relaxed than this STIG, this STIG's requirement will take precedence over the USCYBERCOM directive.

2.1 SECURITY ASSESSMENT INFORMATION

2.1.1 Other STIG Compliance

All other DISA published Security Technical Implementation Guidance (STIG) applicable to the configuration of the system including, but not be limited to, STIGs for the Operating System, Apache (even if the Web GUI is disabled), Database, BIND DNS, etc., must also be validated on the system. The security posture of the system depends upon the system being in compliance with all STIGs.

2.1.2 Manual Review

The STIG documentation included in these packages is written explicitly for the McAfee VSEL 1.9x/2.0x Manual Review. In the event a major version or interim version revision is released from the vendor, either this STIG will be updated with pertinent changes, or a new STIG will be developed.

The Managed Client STIG is intended to be used for Linux systems with the McAfee VirusScan Enterprise for Linux installed via a deployment from the site's McAfee HBSS ePolicy Orchestrator (ePO) server and for which the policy settings have been deployed to the Linux system via the McAfee HBSS ePO server. The Managed Client McAfee Checks and Fixes will be validated/made through the McAfee ePO console.

The Local Client Configured STIG is intended to only be used for Linux systems with McAfee VirusScan Enterprise for Linux installed locally and for which the installation is segregated from the Local Area Network, cannot be managed by a McAfee ePO server, and are not reachable by, nor have access to, the Internet. The Local Client McAfee checks and fixes will be validated/made by the McAfee Web GUI and/or the command line commands and/or by reviewing/modifying the text-based configuration files.

Only standalone Linux systems are permitted to have the McAfee Web GUI enabled.

When navigating the McAfee Web GUI for validating Check Content or applying Fix Text, several pages within the interface, where settings can be changed, have an **Edit** button at the top right of the page. To make changes to the settings on that page, click **Edit**. After making changes, click **Apply** to save the changes.

Some STIG ID Fix Text may not specify the step to click on the **Edit** button, or may not specify the step to click **Apply**.

Refer to the McAfee VSEL Product Guides, Section 3 “VirusScan Enterprise for Linux interface”, for further guidance in applying STIG Fixes through the McAfee VSEL Web GUI.

3. GENERAL SECURITY REQUIREMENTS

3.1 McAfee VirusScan Enterprise for Linux 1.9x/2.0x

3.1.1 Malware protection for Linux systems

Although most malware threats attack Microsoft Windows systems, some malware specifically targets the Linux platform. Protecting these systems becomes important, especially where critical applications are installed on the Linux platform, requiring high availability.

McAfee VirusScan Enterprise for Linux software provides always-on, real-time anti-malware protection for Linux environments. Its Linux-based on-access scanner constantly monitors the system for potential attacks. Regular automatic updates from McAfee Labs protect from the latest threats without requiring system reboot. The software is automatically updated and centrally managed from the McAfee HBSS ePO server.

3.1.2 Proactive Global Protection

Linux-based systems are often in mixed operating system environments, providing advantages but posing security risks to the infrastructure. Unprotected Linux systems may act as carriers, allowing viruses and malware intended to disrupt non-Linux operating systems to move throughout the network. Even after an initial outbreak has been contained, malware may still be able to execute its payload and infect the entire network. McAfee VirusScan Enterprise for Linux software provides extensive proactive protection from viruses, worms, and other malicious code for Linux systems and has been proven to provide 100 percent detection of "in the wild" test samples, plus zero false positives in a selection of clean files. VirusScan Enterprise for Linux software is scalable — designed for today's fast-moving, highly adaptive small- and mid-sized businesses, and global enterprises.

3.1.3 Key Features of McAfee VirusScan Enterprise for Linux (VSEL)

Always-on, on-access scanning - VSEL software provides continuous, on-access anti-malware protection for Linux against malware and other threats.

Heuristic scanning - McAfee scanning technology includes heuristic scanning, which uses behavior-based rules to identify and block new variants of malware without needing to download a signature.

Archive scanning - The McAfee archive scanning function detects and blocks viruses hidden within archived files, providing more complete anti-malware protection for Linux.

Automatic updating - By automating the update process, McAfee frees up IT resources and ensures that the most current updates are always in place. Updates are done behind the scenes and do not require a system reboot.

Cross-platform protection - VSEL software meets real-world needs, including heterogeneous system environments. The anti-malware protection is effective against various types of Windows malware that try to pass through to a Linux system.

Enterprise management and reporting - The software can be centrally managed from a single console with the McAfee ePO platform, enabling management of the entire endpoint security.

Kernel module versioning - On-access scanning on new kernels without the need to recompile modules saves time and effort when rolling out new Linux kernels.

Runtime kernel module - Automatically supports the latest distribution, saving both time and effort. On-access scanning without kernel modules for kernels 2.6.38 with Fanotify (file access notification) ensures Linux is always protected even after kernel updates.

4. NIST GUIDANCE FOR MALWARE HANDLING

The McAfee VSEL 1.9x/2.0x settings have been developed, in part, based on guidance in *NIST 800-83, Guide to Malware Incident Prevention and Handling.*

Excerpt:

Organizations should develop and implement an approach to malware incident prevention.

Organizations should plan and implement an approach to malware incident prevention based on the attack vectors that are most likely to be used, both currently and in the near future. Because the effectiveness of prevention techniques may vary depending on the environment (i.e., a technique that works well in a managed environment might be ineffective in a non-managed environment), organizations should choose preventive methods that are well suited to their environment and systems. An organization's approach to malware incident prevention should incorporate policy considerations, awareness programs for users and information technology (IT) staff, and vulnerability and threat mitigation efforts.

Organizations should ensure that their policies support the prevention of malware incidents.

An organization’s policy statements should be used as the basis for additional malware prevention efforts, such as user and IT staff awareness, vulnerability mitigation, and security tool deployment and configuration. If an organization does not state malware prevention considerations clearly in its policy, it is unlikely to perform malware prevention activities consistently and effectively. Malware prevention-related policy should be as general as possible to allow flexibility in policy implementation and to reduce the need for frequent policy updates, but should also be specific enough to make the intent and scope of the policy clear. Malware prevention-related policy should include provisions related to remote workers, both those using systems controlled by the organization and those using systems outside of the organization's control (e.g., contractor computers, employee home computers, business partner computers, and mobile devices).

Organizations should incorporate malware incident prevention and handling into their awareness programs.

Organizations should implement awareness programs that include guidance to users on malware incident prevention. All users should be made aware of the ways that malware spreads, the risks that malware poses, the inability of technical controls to prevent all incidents, and the importance of users in preventing incidents. Awareness programs should also make users aware of the policy and procedures that apply to malware incident handling, such as how to detect malware on a computer, how to report suspected infections, and what users might need to do to assist incident handlers. In addition, the organization should conduct awareness activities for IT staff involved in malware incident prevention and provide training on specific tasks.

Organizations should have vulnerability mitigation capabilities to help prevent malware incidents.

Organizations should have documented policy, processes, and procedures to mitigate operating system and application vulnerabilities that malware might exploit. Because vulnerabilities usually can be mitigated through one or more methods, organizations should use an appropriate combination of techniques, including patch management, application of security configuration guides and checklists, and additional host hardening measures so that effective techniques are readily available for various types of vulnerabilities.

Organizations should have threat mitigation capabilities to assist in containing malware incidents.

Organizations should perform threat mitigation efforts to detect and stop malware before it can affect its targets. The most commonly used threat mitigation technical control is antivirus software; NIST strongly recommends that organizations deploy antivirus software on all systems for which satisfactory antivirus software is available. To mitigate spyware threats, either antivirus software with the ability to recognize spyware threats or specialized spyware detection and removal utilities should be used on all systems for which satisfactory software is available. Additional technical controls that are helpful for malware threat mitigation include intrusion prevention systems, firewalls, routers, and certain application configuration settings. The System and Information Integrity family of security controls in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, recommends having malware and spyware protection mechanisms on various types of hosts, including workstations, servers, mobile computing devices, firewalls, e-mail servers, and remote access servers.

Organizations should have a robust incident response process capability that addresses malware incident handling.

As defined in NIST Special Publication 800-61, Computer Security Incident Handling Guide, the incident response process has four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity.

Organizations should establish malware incident prevention and handling capabilities that address current and short-term future threats.

Because new malware threats arise constantly, organizations should establish malware incident prevention and handling capabilities that are robust and flexible enough to address both current and short-term future threats and that can be modified and built on to address long-term future threats. Both malware and the defenses against malware continue to evolve, each in response to improvements in the other. For this reason, organizations should stay up-to-date on the latest types of threats and the security controls available to combat each type. As a new category of threats becomes more serious, organizations should plan and implement appropriate controls to mitigate it. Awareness of new and emerging threats and protective capabilities should be part of every organization’s efforts to prevent malware incidents.