Mitel Standard Linux Security Technical Paper

Summary:	This document addresses some commonly asked questions about Mitel Standard Linux (MSL) security
Posted Date:	January 24, 2024.
Audience:	Mitel Sales, Partners, and Customers
Revision Version:	1.4
Revision Reason:	Updated for MSL Release 12.0

Table of Contents

Purpose

Mitel takes data security seriously in protecting the confidentiality, integrity, and availability of customers' data and recognizes security as a crucial aspect of our systems. The purpose of this whitepaper is to provide Mitel customers with an overview of the security features that are inherent in the Mitel Standard Linux (MSL) release 12.0 operating system as well as recommendations for a secure deployment.

Introduction

Mitel Standard Linux (MSL) is an operating system and server solution for single-site and branch-based enterprises. MSL provides a base for a suite of managed services and applications delivered from the Mitel Applications Management Center (AMC) or available on CD/DVD.

MSL is a 64 bit Linux distribution for Intel based computers that is available for download from the Mitel Software Download Center. MSL is based upon the Rocky 8 distribution.

Shared Responsibility Model

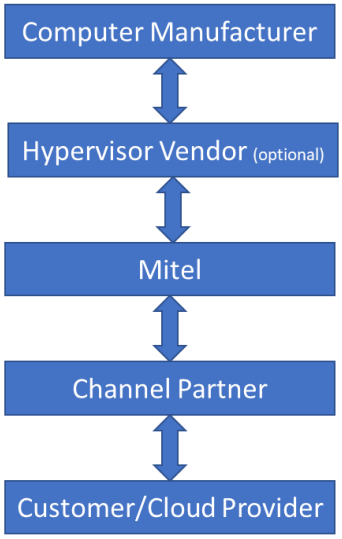

Figure 1: Shared Responsibility Model

Security is a shared responsibility, and this shared responsibility model is also applicable to applications that utilize MSL. Security responsibilities are shared between:

- the computer manufacturer (including BIOS)
- the Hypervisor vendor (if applicable),
- Mitel as the provider of MSL,
- the Partner for configuration and deployment of the solution
- and, when an onsite deployment, the customer to ensure that the network placement is secure; management of their user account(s) and access; and that the solution meets any of their compliance requirements.
    - In a cloud deployment the server placement is the responsibility of the cloud provider

Server Placement

MSL may host many applications with very different features and different network deployment requirements.

For example, the MiVoice Border Gateway application is designed to access the public Internet, however it must not be directly connected to the Internet. To access the Internet, MiVoice Border Gateway must connect to the Internet via a properly configured firewall, or MiVoice Border Gateway must reside inside a firewall DMZ.

Other MSL hosted applications such as the Mitel call controls (e.g. MiVoice Business), collaboration and presence tools (e.g. MiCollab) are designed to operate within the enterprise LAN.

Security best practices for secure deployment of applications designed to operate within the enterprise LAN are that they be correctly configured and be installed behind a firewall on the host MSL server.

Enterprise and Internet Connected Applications Co-Resident on MSL

In situations where enterprise applications (e.g. MiVoice Business) and applications designed to connect to the public Internet (e.g. MiVoice Border Gateway) are co-resident on the MSL server, the MiVoice Border Gateway application must connect to the Internet via a properly configured firewall.

It should be noted that in this scenario the multi-application MSL server has one Network Interface that connects to the LAN to support connectivity to UC applications, and a second Network Interface for providing connectivity to the Internet via the Internet firewall. An additional level of security could be provided by installing a separate MiVoice Border Gateway between the multi-application MSL server and the Internet firewall.

Physical Security

Physical access to the MSL server and underlying network infrastructure should be restricted to only authorized personnel. In the case of an onsite solution ensuring physical access security of the infrastructure is the customer's responsibility. When MSL is part of a cloud solution physical access is the responsibility of the cloud provider.

Installing MSL Onto A Server

To install MSL on a physical server a disc (DVD) or USB media type is required for initial implementation of the operating system. Once MSL has been installed all updates are available online via the Mitel software Download Center.

Mitel therefore recommends that after initial installation that the boot from disc and boot from USB option in the BIOS or UEFI are disabled on the host server.

Password Protecting the GRUB Bootloader

The GRUB (Grand Unified Bootloader) is the first program loaded into memory by the BIOS and is loaded from the hard drive's master boot record when the host machine is switched on. For additional security the GRUB bootloader can be password protected by the administrator.

This can be achieved by executing, as root, the grub-crypt command which generates a hashed password and then copying the output to /etc/grub.conf.. On reboot a user will no longer be able to modify the GRUB boot menu without entering the correct password. The grub bootloader password will survive an upgrade of the operating system. but will be lost if a fresh install is performed.

Firewall Rules

Current versions of MSL use the Mitel Software Download Center to download software updates and applications. The Mitel Software Download Center is a global content distribution network that increases speed and reliability of downloads. The following connections must be allowed through any firewall as a result:

License entitlement:

To register.mitel-amc.com 216.191.234.91 port 22 from the MSL server

To sync.mitel-amc.com 216.191.234.91 port 22 from the MSL server

Access token for content delivery network:

To swdlgw.mitel.com 99.81.17.20 port 443 (occurs during available blade software list update) from the MSL server

Content delivery/blades Akamai

To swdl.mitel.com port 443 (IP address based on location) from the MSL server

Administration Access

Secured, encrypted access using HTTPS to the MSL server is limited to only configured hosts/networks during implementation.

The Administrator password (or System password) is used to access the Server Manager web administration page and the server console as the "admin" user and the Linux shell as the "root" user. A secure, non-trivial password that is at least eight characters in length must be used for new installations. After the password is entered and confirmed MSL examines the password for strength. If it is found to be weak the user is notified and provided the chance to change it.

Server Manager login is protected from brute force password attacks. By default, six consecutive failed login attempts within a 10-minute period locks out the IP address of the client for 30 minutes.

Remote Management

Remote management allows hosts on the specified IPv4 or IPv6 remote network(s) to access the Server Manager of the MSL server. Remote management is disabled by default and must be enabled. This can be limited to an individual host level or a range of IP addresses using network IP address and subnet mask to enable remote management access.

Secure Shell Settings

Secure Shell (SSH) is disabled by default, but if desired can be enabled and be limited to specific networks and/ hosts who can access via SSHv2. Once enabled. SSH provides a secure, encrypted way to log in to the MSL server from a remote location.

Password Rules

When first installing MSL there is no default password and it must be setup during the initial configuration. A secure, non-trivial password that is at least eight characters in length is required.

MSL allows the primary administrator to customize their own password complexity rules including non-alphanumeric requirements, minimum length, uppercase, lowercase and consecutive characters requirements as well as forbidden words to use as a password.

The locally stored password for the root and admin accounts are hashed using the SHA-512 algorithm using a random salt value 8 characters in length.

Audit Trails

Access to the MSL server is logged based on time of day, IP address, log-in IDs.

Audit trails are supported for installed application to maintain records of data processing activities. All changes made via the administrator accounts are logged to the Audit Log. The audit log may be sent through syslog to a central site for aggregation and analysis. The audit log contains the IP address, administrator name or application token identifier, information on which objects were added/changed/removed, and the details of that operation.

The Audit Log can be accessed only by the administrator unless it has been sent to another server by syslog.

MSL Hardening

The MSL operating system as noted previously in this document is based upon the Rocky 8 operating system when deployed on Intel based architecture computers.

Note: Power PC platforms such as the 3300 ICP CX II and MXe III platform use a different Linux distribution from Wind River.

Operating system hardening of MSL employs the following techniques to minimize any vulnerabilities and reduce the potential attack surface of an MSL server.

Unnecessary Services and Applications are Removed or Disabled

Mitel reduces the potential attack surface of the operating system by removing unnecessary services and applications that the Mitel applications do not make use of including:

- Unnecessary IP Ports are closed
- Wireless and Bluetooth networking services are not included
- Email client and Web browser are not included
- Remote control and access is disabled by default, with common unsecured services removed, e.g. Telnet
- Directory services are disabled by default
- Web Servers and services are only available to customer defined trusted networks and / or hosts. Access control is part of the implementation process and can only be updated by authorized admin
- Software development tools and compilers are not provided
- File and printer sharing services, NETBIOS, NFS, FTP, etc. are disabled or removed, if not needed
- SNMP is disabled by default. SNMPv3 and SNMPv2c are supported if enabled by an authorized admin.

Operating System User Authentication

- Default accounts and non-interactive accounts are removed or disabled
- Automated time synchronization is provided via NTP
- There is no default password – it must be configured during installation. The password is subject to length and complexity rules. Customer can define their own rules.
- Password policy, and new users, requires use of a strong password policy (min password length, mix of characters and symbols). Customer can define their own complexity rules.
- Remote access on external interfaces is disabled by default
- Repeat failed access attempts are black-listed after 6 attempts within 10 minutes for 30 minutes, from server manager remote access (when enabled)
- Repeat failed access attempts are black-listed after 10 attempts from SSH remote access (when enabled)
- SNMP is owned by root, not administrators
- Login and Logout activity of users and root are logged

Resource Controls

- MSL does not provide any world writable permissions
- MSL does not provide any 'no-owner' files
- Host based firewalls are enabled and configured
- External interfaces do not report server type, nor release version
- Only necessary IP ports are enabled by the OS so manual port intervention is not necessary.
- Prior to MSL Release 12.0, TLS 1.0 is disabled by default on server manager port 443 (TLS 1.1 can also be disabled by an authorized administrator)
- At MSL Release 12.0, TLS v1.0 and TLS v1.1 are no longer supported

Access Controls

Access control mechanisms restrict user access, including, but are not limited to:

- Password files and hash files
- Logs and system audit files
- Server content files
- Server and configuration files

The combination of access controls, resource controls, OS User Authentication and the disabling or removal of unnecessary services means that MSL has a much reduced possibility of being the subject of unauthorized access and an attack by a bad actor.

Vulnerability Scanning and Penetration Testing

Mitel tests for vulnerabilities and performs penetration testing as part of the standard quality assurance programs within Mitel. Product releases and patches are scanned for vulnerabilities prior to public release. Test tools are maintained with current known vulnerabilities signatures.

Mitel does, however, recommend that customer installations should carry out their own periodic vulnerability and penetration easting of their deployed solution. Mitel security vulnerabilities are reported through the standard technical support process via the customers channel partner.

Encryption technologies

Data in Transit

Prior to MSL Release 12.0, Data in transit is encrypted, with different security levels – TLS v1.1, and TLS v1.2 only. TLS v1.0 is supported for backwards compatibility but is disabled by default.

At MSL Release 12.0, data in transit is encrypted, with either TLS v1.2 or TLS v1.3.

Data at Rest

Password information is hashed, however general disk encryption is not provided. Where possible Mitel recommends the use of virtualization with the MSL server virtual hard drive deployed on a Storage Area Network (SAN) that is encrypted at the SAN and/or virtual machine level.

Certificates

An SSL/TLS web server certificate authenticates the identity of a web site and encrypts information passed between the web server and the web client using Transport Layer Security (TLS) technology. A default self-signed SSL certificate is provided with the MSL server. For enhanced security and ease of use, a customer may obtain a signed SSL certificate from a third-party Certificate Authority (CA). Two options are available:

- Let's Encrypt: - is a free, automated, and open Certificate Authority. It enables a customer to obtain a Domain Validated SSL certificate simply by providing your domain settings and then clicking a button. The acquired certificate is monitored and renewed automatically. More information about Let’s Encrypt is available at https://letsencrypt.org/docs/ .
- Other 3rd-Party: An alternative third-party Certificate Authority issues an Extended Validation SSL certificate upon request, typically for a fee. Companies such as Entrust and GoDaddy provide such services. To obtain a generic SSL certificate, you must first generate a Certificate Signing Request (CSR) on the MSL system and send it to the CA. The CA will then return a package containing your web server certificate, plus any intermediate certificates that are required to maintain the certificate key chain. Supported formats for importing third-party SSL certificates are either PEM or PKCS#12 format. Certificates and keys must use the RSA algorithm

Cipher Suites

MSL uses OpenSSL for Transport Layer Security (TLS) 1.3 and 1.2support. The version of OpenSSL varies between MSL versions. An authorized administrator may view the OpenSSL version by running the following

Linux command "***openssl version***". For example, OpenSSL 1.0.2k-fips 26 Jan 2017 and will vary from release to release.

To see the OpenSSL cipher suites supported use the command "***openssl ciphers"***

Anti-Virus Protection

While the use of antivirus software is widely accepted in the IT industry for use on servers, end user mobile platforms and desktops, running antivirus software on a real-time computing platform is problematic and the applications that MSL hosts are real time application such as VoIP call controls, Session Border Controllers and other voice processing applications.

Applications that process data in real-time require unfettered access to processor resources, memory systems, disk drive accesses and network communications. When Mitel applications are deployed on industry standard servers or virtual machines, as per the application's engineering guidelines, the machine's resources will have been sized to ensure that the applications will have unrestricted and timely access to the resources that they require.

Since MSL is hosting real time application and these real-time data processing applications are executing on carefully sized computing platforms, the installation of antivirus software is not currently recommended.

Mitel cannot guarantee that third party antivirus software will not affect the performance of the hosted real time application. Therefore, Mitel does not offer any endorsements of antivirus software vendors, or evaluations of particular antivirus products. Should a customer require technical support from Mitel related to a system that has antivirus software installed, Mitel may require that the software be removed before Mitel can start troubleshooting the problem.

In addition, MSL is a hardened Linux distribution (as described elsewhere in this document) with a limited attack surface. It does not provide Windows services, nor proxies Windows services.

Other security threats are actively monitored with any patches and upgrades provided as necessary, in a timely manner.

Endpoint Protection

There are now Endpoint Protection solutions available that require far less compute resources than antivirus solutions and when there are adequate compute resources provisioned on the servers, Endpoint Protection solutions can be used to secure real time severs without impacting the quality of the real time data.

For further information regarding Endpoint Protection usage with Mitel applications running on MSL servers, refer to the Mitel document Real Time Application Servers and Endpoint Protection, which is available on Mitel's Document Center Web Site.

Software Patch Management Policy

It is necessary for the administrator to ensure that the MSL systems are always updated and equipped with all critical patches to guarantee the highest level of security. Mitel has developed best practices for the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the correct functioning of the system.

Logging

MSL includes a syslog server for message logging. When a system event occurs, such as a failed authentication attempt or login failure, the affected service generates a message which is recorded in a log file. These can be examined by an authorized user.

Functionality can be enabled on the local system to accept syslog messages from remote hosts, provided that they are in a trusted network. And the local system can send its own syslog messages to remote hosts.)

The audit log contains the IP address, administrator name or application token identifier, information on which objects were added/changed/removed, and the details of that operation.

Mitel Security Policy

Public notices regarding moderate and high-risk product security vulnerabilities are published under Security Advisories at https://www.mitel.com/support/security-advisories

The Mitel Product Security Policy is available at https://www.mitel.com/support/security-advisories/mitel-product-security-policy

Mitel Privacy Policy

Mitel's Application Privacy Policy available at https://www.mitel.com/en-ca/legal/mitel-application-privacy-policy.

Additional Mitel Documentation

Additional Mitel application specific documentation can be found at the Mitel document Center at: https://www.mitel.com/document-center