Moxa Industrial Linux

Software Life-cycle Policy

10 November 2023

Introduction

Moxa Industrial Linux (hereinafter referred to as MIL) is an industrial-grade Linux distribution developed by Moxa and released for Moxa computer platforms since 2018. The mission of MIL is to address the long-term system needs of industries, such as power, water, oil and gas, transportation, and factory automation, to make industrial projects secure and sustainable. MIL is based on the Debian distribution and the standard Linux kernel and hence makes it easy to deploy applications on multiple systems. Moxa is working with industry leaders to create a reliable and secure Linux-based embedded software platform. Moxa is a member of The Linux Foundation® and is part of its Civil Infrastructure Platform (CIP) project that aims to create an open-source platform to make industrial projects secure, reliable, scalable, and sustainable.

MIL Releases

MIL is based on the Debian distribution and the standard Linux kernel. Debian announces its new stable release on a regular basis (see the Debian Releases and Debian LTS Wiki pages for details). The illustration and table below provide information on MIL standard and long-term support (LTS) releases. The support duration for an LTS release can be divided into three periods: full-support, maintenance, and LTS. Only MIL-eligible products in the Arm-based computing platform family are covered in the LTS period. The support duration for a standard release can be divided into the full-support and maintenance periods.
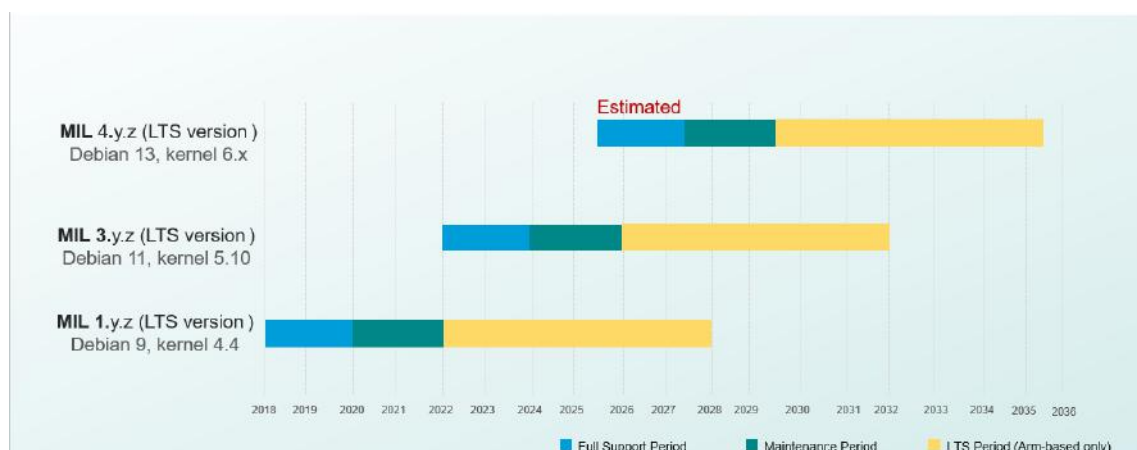

Version	Based On	Release	Full Support	Maintenance	LTS*
V1.x.x (LTS)	Debian 9	2018	until 2019	2020 to 2021	2022 to 2027
V3.x.x (LTS)	Debian 11	2022	until 2023	2024 to 2025	2026 to 2031
V4.x.x (LTS)	Debian 13	2025	until 2027	2027 to 2029	2029 to 2035
		(estimated)	(estimated)	(estimated)	(estimated)

Note: Only MIL-eligible products in the Arm-based computing platform family are covered in the LTS period.

Moxa reserves the right to change the terms and conditions of the service policy at any time. Check the latest policy document at www.moxa.com.

Revisions

MIL releases use versions in the **X.Y.Z** format where **X** represents the MIL generation release, **Y** represents the major release, and **Z** represents the minor release. Software changes can be released individually on an as-needed basis or aggregated into a minor release, which may also contain security and bug fixes. Between major releases, all software changes (including new feature enhancements, updates/fixes released as part of a minor release, and any patch sets) will be cumulatively applied to the latest MIL release.
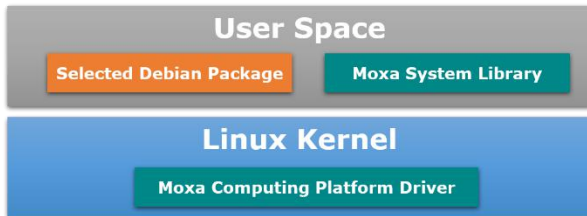
Security fixes and bug fixes* could be released for:

- The Linux kernel
- The Linux device driver (used in Moxa computing platforms)
- Selected Debian packages in the user space (refer to the supplement **Debian LTS Package List**)
- Moxa system library

Note: Unless the bootloader has a critical bug or security vulnerability, no bootloader upgrade will be included in a patch.

Release cadence of each MIL generation is once or twice per year. All released software changes will be available in the Moxa Debian repository throughout the MIL life cycle.

Full Support Period

The full support period starts when a MIL generation version is released and ends two years thereafter. Moxa provides the following services during the full-support period.

- Qualified, critical, and important security fixes and selected high-priority bug fixes will be released as they become available.
- Moxa may provide new or improved hardware-enablement functionality and selected software functionality enhancements as major or minor releases at its sole discretion.
  - The releases are cumulative and include the contents of previously released updates. The focus for the releases during this phase will be on resolving defects that are of high and medium priority.
- Hardware-enablement functionalities that do not require substantial software changes may be provided independent of minor releases at Moxa's sole discretion.

Maintenance Period

The maintenance period starts when the full-support period is completed and ends two years thereafter. Moxa provides the following services during the maintenance period.

- Additional software changes may be delivered as minor releases and on an as-needed basis.
  - The minor releases will also include available and qualified software changes for security vulnerabilities.
  - Minor releases are cumulative and include the contents of previously released updates. The focus of the minor releases during this phase will be on resolving defects that are of high or medium priority.
- New software functionalities will not be available during this phase.

LTS Period

The LTS period starts when the maintenance period is completed and ends six years thereafter. Moxa may at its sole discretion provide the same services as the maintenance period only for MIL-eligible products of the Arm-based computing platform family during this period.

- The same services as the maintenance period provided at Moxa's sole discretion.
- New software functionalities will not be available during this phase.

After the Support Period Ends

The support period ends when the maintenance period of standard releases ends or the LTS period of LTS releases ends. No technical support will be provided after the end of the support period. And, in no event will bug fixes, security fixes, hardware enablement, and root-cause analysis be available during this phase. Please contact your local sales representative if you would like to avail services beyond the support scope defined herein. A support fee may apply based on the support scope to be defined in a service contract with Moxa.

Support Policy

Standard Releases

Moxa provides 4-year support for MIL standard releases, including a 2-year full support period and a 2-year maintenance period.

LTS Releases

Moxa provides 10-year support for MIL LTS releases, including a 2-year full support period, a 2-year maintenance period, and a 6-year LTS period.

Fixes to Security Vulnerabilities

When a security vulnerability is reported, Moxa Product Security Incident Response Team (PSIRT) will evaluate the CVSS (Common Vulnerability Scoring System) score of the vulnerability using the CVSS calculator and considering additional factors, such as temporal and environmental metrics to reflect a more accurate measurement of the severity.

Note: CVSS Score shown in NIST database is the base score that only represents a general severity measure. It offers an initial indication of a vulnerability's intrinsic risk factors without taking into account any environmental or temporal factors.

Moxa will respond to the reported vulnerability within 14 days with impact analysis, mitigation plan, and the date on which a mitigation solution can be provided based on the following guidance:

- If the evaluated CVSS (Common Vulnerability Scoring System) score is equal or greater than 7.0 (high risk), Moxa will provide the mitigation solution within 30 calendar days.
- If the evaluated CVSS (Common Vulnerability Scoring System) score is between 4.0 and 6.9 (medium risk), Moxa will provide the mitigation solution within 90 calendar days.
- If the evaluated CVSS (Common Vulnerability Scoring System) score is below 4.0 (low risk), Moxa will provide the mitigation solution within 120 calendar days.
- In some exceptional and unexpected circumstances, Moxa may not be able to release the mitigation solution for vulnerabilities within the aforementioned days. Moxa reserves the right to extend the delivery time.

The mitigation solution may be in the form of but not limited to one of these methods:

- Security Advisories available on the Moxa official website that include a description of the vulnerability, workaround, solutions, and/or installation instructions.
- Patches available in the Moxa Debian repository for all affected products.

Moxa provides RSS feed of Security Advisories for all Moxa products. Please subscribe to these feeds and receive notifications of new patches via your RSS reader. Moxa also provides a process for customers to report security vulnerabilities. If you are concerned about a potential security vulnerability in a MIL release, please report it via our website.

References

1. Debian website (Link)
2. Debian Package Management (Link)
3. Debian Security Bug Tracker (Link)
4. The Linux Foundation (Link)
5. Common Vulnerability Scoring System (Link)

Supplement—Debian LTS Package List

MIL v1.0—Selected Debian Packages

Source Package	Binary Package		
acl	libacl1		
adduser	adduser		
apparmor	libapparmor1		
apr	libapr1		
apr-util	libaprutil1	libaprutil1-dbd-sqlite3	libaprutil1-ldap
apt	apt	apt-utils	libapt-inst2.0
	libapt-pkg5.0		
attr	libattr1		
audit	libaudit1	libaudit-common	
autogen	libopts25		
base-files	base-files		
base-passwd	base-passwd		
bash	bash		
bc	bc		
bind9	libdns-export162	libisc-export160	
bluez	bluez		
boost1.62	libboost-filesystem1.62.0	libboost-system1.62.0	
bridge-utils	bridge-utils		
bsdmainutils	bsdmainutils		
busybox	busybox	udhcpc	
bzip2	libbz2-1.0		
ca-certificates	ca-certificates		
can-utils	can-utils		
cdebconf	libdebconfclient0		
cgmanager	cgmanager	libcgmanager0	
coreutils	coreutils		
cpio	cpio		
crda	crda		
cron	cron		
cryptsetup	libcryptsetup4		
curl	curl	libcurl3	libcurl3-gnutls
cyrus-sasl2	libsasl2-2	libsasl2-modules-db	
dash	dash		
db5.3	libdb5.3		

Source Package	Binary Package		
dbus	dbus	libdbus-1-3	
debconf	debconf	debconf-i18n	
debian-archive-keyring	debian-archive-keyring		
debianutils	debianutils		
diffutils	diffutils		
dpkg	dpkg		
e2fsprogs	e2fslibs	e2fsprogs	libcomerr2
	libss2		
elfutils	libelf1		
ethtool	ethtool		
expat	libexpat1		
findutils	findutils		
firmware-nonfree	firmware-atheros	firmware-misc-nonfree	
gawk	gawk		
gcc-6	gcc-6-base	libgcc1	libstdc++6
gdbm	libgdbm3		
glib2.0	libglib2.0-0		
glibc	libc6	libc-bin	libc-l10n
	locales	multiarch-support	
gmp	libgmp10		
gnupg2	gnupg	gnupg-agent	gpgv
gnutls28	libgnutls30		
gpm	libgpm2		
grep	grep		
gzip	gzip		
hostname	hostname		
i2c-tools	i2c-tools		
icu	libicu57		
ifenslave	ifenslave-2.6	ifenslave	
ifupdown	ifupdown		
init-system-helpers	init	init-system-helpers	
iperf3	iperf3	libiperf0	
iproute2	iproute2		
iptables	iptables	libip4tc0	libip6tc0
	libiptc0	libxtables12	
iputils	iputils-ping		
isc-dhcp	isc-dhcp-client	isc-dhcp-common	

Source Package	Binary Package		
iw	iw		
jansson	libjansson4		
jq	jq	libjq1	
json-c	libjson-c3	libjson-c-dev	
keyutils	libkeyutils1		
kmod	kmod	libkmod2	
krb5	libgssapi-krb5-2	libk5crypto3	libkrb5-3
	libkrb5support0		
libassuan	libassuan0		
libatasmart	libatasmart4		
libbsd	libbsd0		
libcap2	libcap2		
libcap-ng	libcap-ng0		
libedit	libedit2	libestr0	
libevent	libevent-2.0-5		
libfastjson	libfastjson4		
libffi	libffi6		
libgcrypt20	libgcrypt20		
libgpg-error	libgpg-error0		
libgudev	libgudev-1.0-0		
libidn2-0	libidn2-0		
libidn	libidn11		
libksba	libksba8		
liblocale-gettext-perl	liblocale-gettext-perl		
liblogging	liblogging-stdlog0		
liblognorm	liblognorm5		
libmbim	libmbim-glib4	libmbim-proxy	
libmnl	libmnl0		
libnetfilter-conntrack	libnetfilter-conntrack3		
libnfnetlink	libnfnetlink0		
libnih	libnih1	libnih-dbus1	
libnl3	libnl-3-200	libnl-genl-3-200	
libonig	libonig4		
libpcap	libpcap0.8		
libpipeline	libpipeline1		
libpsl	libpsl5		
libqmi	libqmi-glib5	libqmi-proxy	libqmi-utils

Source Package	Binary Package		
libseccomp	libseccomp2		
libselinux	libselinux1		
libsemanage	libsemanage1	libsemanage-common	
libsepol	libsepol1		
libsigsegv	libsigsegv2		
libssh2	libssh2-1		
libtasn1-6	libtasn1-6		
libtext-charwidth-perl	libtext-charwidth-perl		
libtext-iconv-perl	libtext-iconv-perl		
libtext-wrapi18n-perl	libtext-wrapi18n-perl		
libunistring	libunistring0		
libxml2	libxml2		
lldpd	lldpd		
lm-sensors	libsensors4		
logrotate	logrotate		
lsb	lsb-base		
lua5.2	liblua5.2-0		
lvm2	dmsetup	libdevmapper1.02.1	
lz4	liblz4-1		
lzo2	liblzo2-2		
mawk	mawk		
mime-support	mime-support		
mpfr4	libmpfr4		
mtd-utils	mtd-utils		
nano	nano		
ncurses	libncurses5	libncursesw5	libtinfo5
	ncurses-base	ncurses-bin	
netbase	netbase		
net-snmp	libsnmp30	libsnmp-base	snmp
	snmpd		
nettle	libhogweed4	libnettle6	
net-tools	net-tools		
newt	libnewt0.52	whiptail	
nghttp2	libnghttp2-14		
npth	libnpth0		
ntp	ntp		
openldap	libldap-2.4-2	libldap-common	

Source Package	Binary Package		
openssh	openssh-client	openssh-server	openssh-sftp-server
openssl1.0	libssl1.0.2		
openssl	libssl1.1	openssl	
p11-kit	libp11-kit0		
pam	libpam0g	libpam-modules	libpam-modules-bin
	libpam-runtime		
parted	libparted2	parted	
pciutils	libpci3		
pcre3	libpcre3		
pcsc-lite	libpcsclite1		
perl	libperl5.24	perl	perl-base
	perl-modules-5.24		
pinentry	pinentry-curses		
policykit-1	libpolkit-agent-1-0	libpolkit-gobject-1-0	
popt	libpopt0		
ppp	ppp		
procps	libprocps6	procps	
readline	libreadline7	readline-common	
rsyslog	rsyslog		
rtmpdump	librtmp1		
sed	sed		
sensible-utils	sensible-utils		
shadow	login	passwd	
slang2	libslang2		
sqlite3	libsqlite3-0		
sudo	sudo		
sysstat	sysstat		
systemd	libpam-systemd	libsystemd0	libudev1
	systemd	systemd-sysv	udev
systemd-shim	systemd-shim		
sysvinit	sysvinit-utils		
tar	tar		
tasksel	tasksel	tasksel-data	
tcp-wrappers	libwrap0		
tzdata	tzdata		
u-boot	u-boot-tools		
ucf	ucf		

Source Package	Binary Package		
udisks2	libudisks2-0	udisks2	
ustr	libustr-1.0-1		
util-linux	bsdutils	libblkid1	libfdisk1
	libmount1	libsmartcols1	libuuid1
	mount	util-linux	
vim	vim	vim-common	vim-runtime
	xxd		
wget	wget		
wireless-regdb	wireless-regdb		
wpa	wpasupplicant		
wvdial	wvdial		
wvstreams	libuniconf4.6	libwvstreams4.6-base	libwvstreams4.6-extras
xapian-core	libxapian30		
xz-utils	liblzma5	xz-utils	
zlib	zlib1g		