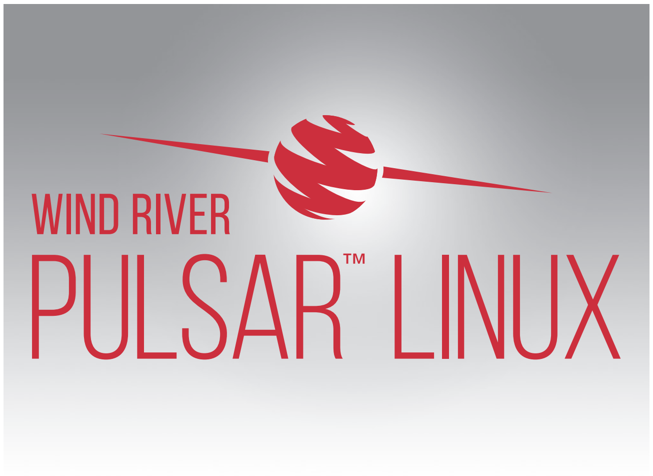
WIND RIVER PULSAR LINUX

Container-based Operating System



Features

- Security Vulnerability Protection
- Open Source Software Compliance Artifacts
- Customized Base Platform
- Extensibility via packages and/or containers
- Enabled IoT Connectivity Protocols

Introduction

Wind River® Pulsar™ Linux is a container-based operating system designed to deliver a steady flow of bug fixes and security vulnerability fixes to protect deployed devices and mitigate cost of ownership and risks associated with unmanaged open source technology. Using the Yocto Project as a technology base, Pulsar delivers vital components for the productization and commercialization of Internet of Things (IoT) devices, such as update capabilities during development and post-deployment, continuous security monitoring and vulnerability protection, and IP and export compliance artifacts. Designed to be simple to download and develop on, Pulsar provides a ready-to-use binary image for specific hardware. It includes selected packages and middleware from the traditional Wind River Linux and market-specific profiles.

Feature Details

Security Vulnerability Protection

The Pulsar distribution is kept up to date and protected against security attacks through constant regular maintenance with security patches and critical Linux updates pulled from a Wind River–certified repository through a secure channel. Fixes to known security vulnerabilities are provided throughout the lifecycle of Pulsar devices. The Wind River security team is constantly monitoring security vulnerabilities, including specific security notifications from U.S. government agencies and organizations such as the National Institute of Standards and Technology and the United States Computer Emergency Readiness Team, as well as public and private security mailing lists and the Common Vulnerabilities and Exposures (CVE) database at cve.mitre.org. The team receives alerts from each of these organizations whenever a new security threat arises. Alerts include both community-confirmed and potential vulnerabilities. Wind River mitigates these threats through a four-step approach: monitoring, assessment and prioritization, notification, and remediation.

Open Source Software Compliance Artifacts

Open source provides tremendous benefits to IoT systems. However, building turnkey solutions based on Linux requires thorough licensing review and disclosure. The Pulsar compliance artifacts relieve developers of the burden of identifying, reporting, and complying with hundreds or even thousands of open source software (OSS) license terms. Pulsar reduces the risk and costs of open source adoption with the due diligence provided by a licensing compliance and export disclosure program. Whether it concerns protecting the IP developed on top of the OSS base or clearing export classifications, these issues must be addressed early in the supply chain or there can be costly repercussions for downstream customers - fees and fines, business disruption, even lawsuits. The product comes with a compliance envelope - a zipped archive that contains the following:

- All required licensing data
- Source code legal notices
- Export cryptography information associated with the OSS used to construct the product

Customized Base Platform

Base platform features include:

- Multiple architectures: Certified images run on all major CPU architectures.
- Easy application development and device lifecycle management: Using the available SDK, users can focus directly on developing their own value-added features.
- Quick prototyping: Pulsar is shipped as a pre-installed binary image with hardware or is available for download.
- Integration with cloud tools: Pulsar can run on simulated hardware by accessing a cloud based virtual lab that includes software and hardware simulations.
- Top-to-bottom security: From secure boot to middleware and applications, all transfers are made via a certified repository feed.
- Software updates for deployed devices: A smart update agent connects to certified repositories for updating devices deployed in the field.
- Extensibility via packages: You can add packages on the target from a certified repository or build packages on the target.
- Containers for application middleware abstraction: Pulsar can bring any application from any ecosystem to run on any device, even applications that need their own middleware.
- Free open source software (FOSS) compliance: Source code is provided for power

Enabled IoT Connectivity Protocols

Brand	Model/Advantech P/N	Chip	Type
WiFi+BT			
Advantech	EWM-W158F01E	Atheros AR9592-AR1B	WiFi
Silex	SX-PCEAN2	Atheros AR9580	WiFi
Advantech	EWM-W157H01E	RTL8821AE	WIFI+BT
Advantech	EWM-W163M201E		WIFI+BT
3G+4G module			
Telit	XINTEL-HE910GPSPCI	Telit HE910	3G
Sierra	MC7354: 968EMC0060	Sierra MC7354	3G + GPS
Sierra	MC7430: 968EMC0067	Sierra Wireless AirPrime	3G+GPS
Advantech	EWM-C118HD01E	u-blox SARA-U270	3G
Advantech	EWM-C109F601E	U-blox LISA-U200	3G
Advantech	EWM-C117FL04E	u-blox MPCI-L210	4G
GPS /GNSS module			
Advantech	EWM-G108H01E	u-blox NEO-7	GPS
Advantech	EWM-G109H01E	u-blox NEO-M8N	GPS
Sierra	968EMC0066	Sierra MC7455	4G + GPS
Telit	968EMW0093	Telit HE910	3G
Redpine	TBA	Redpine RS9113	Zigbee+4G+WiFi+BT

Minimum Requirements

Supported target architectures and processor families

- Intel® Atom™ family / Intel® N4200 & E3900 Series