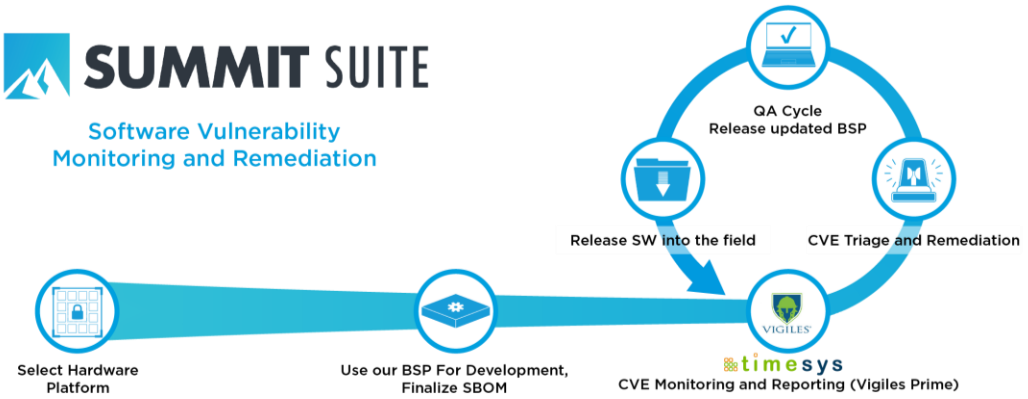
Laird™ CONNECTIVITY

# Summit Suite™ - Software Vulnerability Monitoring and Remediation

## CVE Monitoring and BSP Security Lifecycle Management

## LONG TERM SUPPORT LINUX AND ZEPHYR WITH CVE MONITORING, REPORTING, AND REMEDIATION


SUMMIT SUITE
Software Vulnerability Monitoring and Remediation
QA Cycle
Release updated BSP
Release SW into the field
CVE Triage and Remediation
VIGILES
timesys
Select Hardware Platform
Use our BSP For Development, Finalize SBOM
CVE Monitoring and Reporting (Vigiles Prime)

Day after day, Common Vulnerabilities and Exposures (CVEs) threaten your devices deployed in the field. Managing your devices' boards support package (BSP) for vulnerabilities by yourself is a full-time job: creating custom tools to scan, monitor, and report on the software bill of materials (SBOM) for your device and dedicating engineers to port patches or upgrade software to address never-ending vulnerabilities. It's time consuming and takes critical resources away from developing your core product. Leverage our Summit Suite Software Vulnerability Monitoring and Remediation solution for BSP security lifecycle management from the start to the end.

We start with customized BSPs for our 60 Series SOM, Sentrius™ IG60, and Summit SOM 8M Plus. These BSPs are based on Yocto or Buildroot to generate Linux operating systems for application processors and Zephyr for microcontrollers. Our long-term support of these BSPs help your team keep software up to date while stabilizing a product to get to market launch and maintain it in the field with minimal disruptions and retesting.

Next, we onboard your team and your SBOM into a shared workspace with our FAE / engineering teams in Vigiles Prime, a best-in-class vulnerability monitoring and reporting cloud-based software service provided by our partner Timesys. This helps us track what CVEs affect your software before launch as well as later in the field. Using the industry and government standard Common Vulnerability Scoring System (CVSS), we help you prioritize the most severe vulnerabilities. As your development progresses, we work with you to monitor, report, and triage CVEs found in your SBOM.

We work with you to triage and remediate CVEs related to your SBOM before and after your product goes to market, regularly meeting with your team on joint remediation or mitigation strategies. We then move on those strategies to provide an updated BSP release to address CVEs. If a new QA cycle is required on our BSP and hardware platform combination, our QA team will get to work to ensure our product continues to have the feature and functionality your team expects. Your team can continue to focus on adding value through your expertise and outsource the burden of retesting core BSP functionality.

We're one partner with every needed capability, providing the device hardware, the optimized BSP, BSP vulnerability monitoring, and BSP vulnerability remediation and mitigation under one roof.

- **New Long-Term Support BSPs every two years** – with four biannual releases to each new long-term BSP. Supported for longer or with more frequent releases with our Vulnerability Monitoring and Remediation
- **Industry-leading alerts and reports** – Vigiles Prime CVE reports provide deep detail on vulnerabilities and solutions and help identify the most severe and urgent exposure. They can be exported to share and distribute among key stakeholders within your organization
- **Shared workspace for collaboration with our organization** – Share access with our FAE/engineering teams on identifying vulnerabilities and developing mitigation / remediation strategy.
- **Continuous improvement ahead of the curve** – monitor for vulnerabilities both before and after your device is in the field, fueling a cycle of continuous improvement over decade-long lifecycles

## FEATURES AT A GLANCE

### LONG-TERM SUPPORT BSPS WITH FLEXIBILITY

New long-term BSPs every two years with four biannual updates to each new long-term BSP. Get longer security support windows or more frequent security updates with Summit Suite.

### INDUSTRY-BEST CVE ALERTS, MONITORING, AND REPORTING

New common vulnerabilities are discovered week after week. Keep ahead of the ones affecting your SBOM, with severity highlighting and exportable reports for the rest of your organization.

### SHARED PLATFORM FOR YOUR TEAM AND OURS

Vigiles Prime instance allows our teams to connect on identifying CVEs and enacting solutions. Automatically import your SBOM updates and get scans and reports with Vigiles Prime APIs.

### FOCUS ON WHAT MATTERS MOST – YOUR CORE PRODUCT

Monitoring for CVE remediation is a full-time job. Let us keep you ahead of the curve with industry-standard continuous monitoring using CVSS scoring and updated BSP releases.

### LEVERAGE OUR ENGINEERING AND QA FOR BSP UPDATES & TESTING

We work with you to identify the remediation strategies you need to preserve feature functionality. Our QA teams can coordinate testing to maintain core BSP compatibility.

### INDUSTRY-LEADING SUPPORT

Our Tier 2 and FAE support bring expert assistance, working with you and our engineering to reduce your time to market.

## APPLICATION AREAS

- Smart Buildings and Appliances
- Smart Robots
- Industrial IoT, Vision Systems
- Printers and Scanners
- Medical Devices

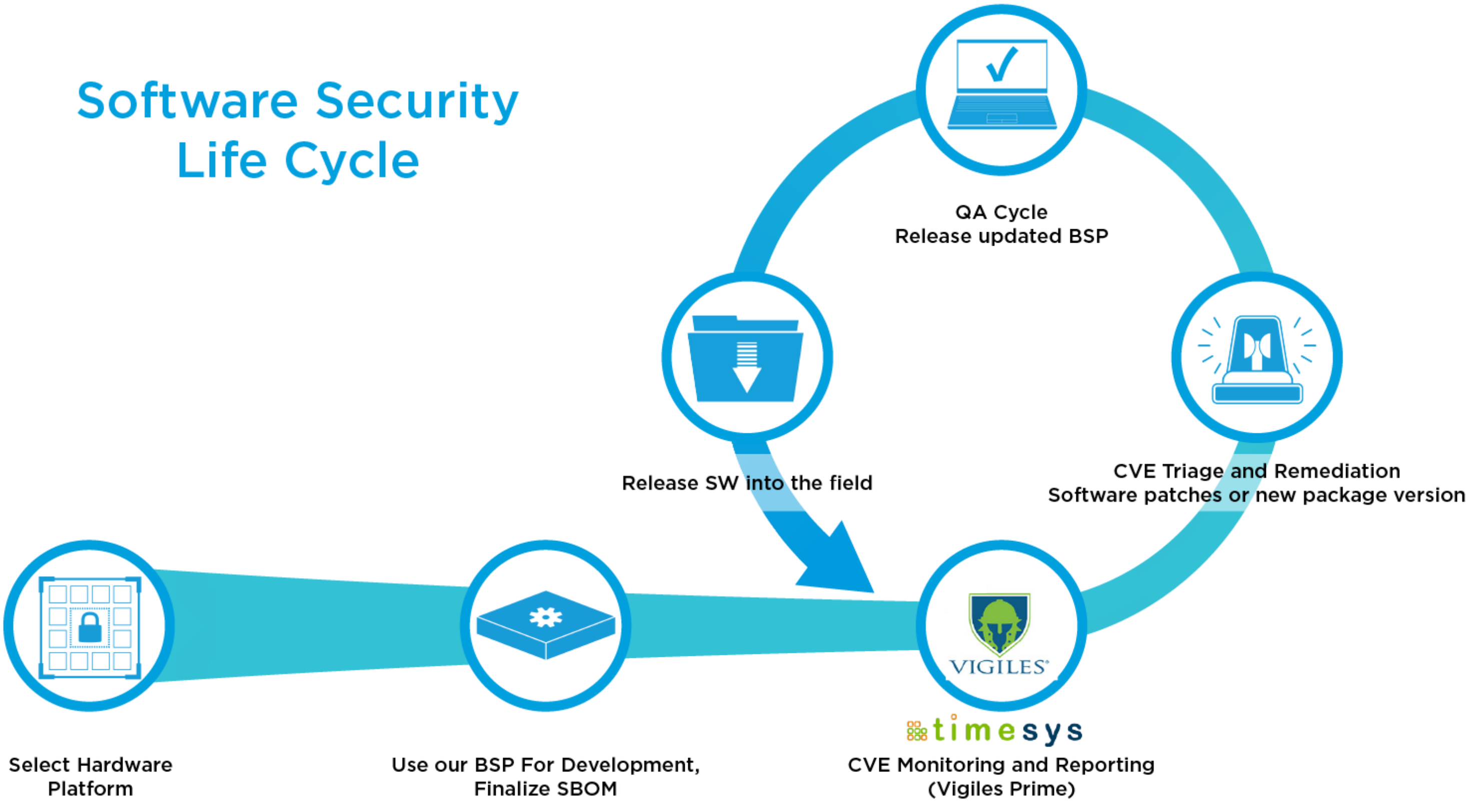
Interested in our Summit Suite?
Visit us at https://www.lairdconnect.com/iot-software/summit-suite

## Long-Term Support BSP Roadmap

Every two years, we release new Linux and Zephyr long-term support (LTS) BSPs for partners using our hardware products. We do 4 standard releases on a 6-month cadence from each new Linux and Zephyr LTS BSP. These form the foundation of the long term BSP security lifecycle. After the 4 standard releases from a Linux and Zephyr LTS BSP, it can be maintained for new security releases under the Summit Suite Vulnerability Monitoring and Remediation solution. If more frequent security releases are desired during the 4 standard release cycle, these security release can also be done under the Summit Suite Vulnerability Monitoring and Remediation solution.

| **Summit Yocto Linux+Zephyr BSP Releases** | 2022 | | | | 2023 | | | | 2024 | | | | 2025 | | | | 2026 | | | | 2027 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| Future Release | | | | | | | | | | | | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ |
| Release 4 – LTS Kernel, LTS Yocto, LTS Zephyr | | | | | | | | | | | | 4 R1 | | 4 R2 | | 4 R3 | | 4 R4 | | Further Releases Summit Suite Only | | | | |
| Release 2 – 5.15 Kernel, Yocto Kirkstone, Zephyr 2.7 | | | | 2 R1 | | 2 R3 | | 2 R4 | | 2 R4 | | Further Releases Summit Suite Only | | | | | | | | | | | | |

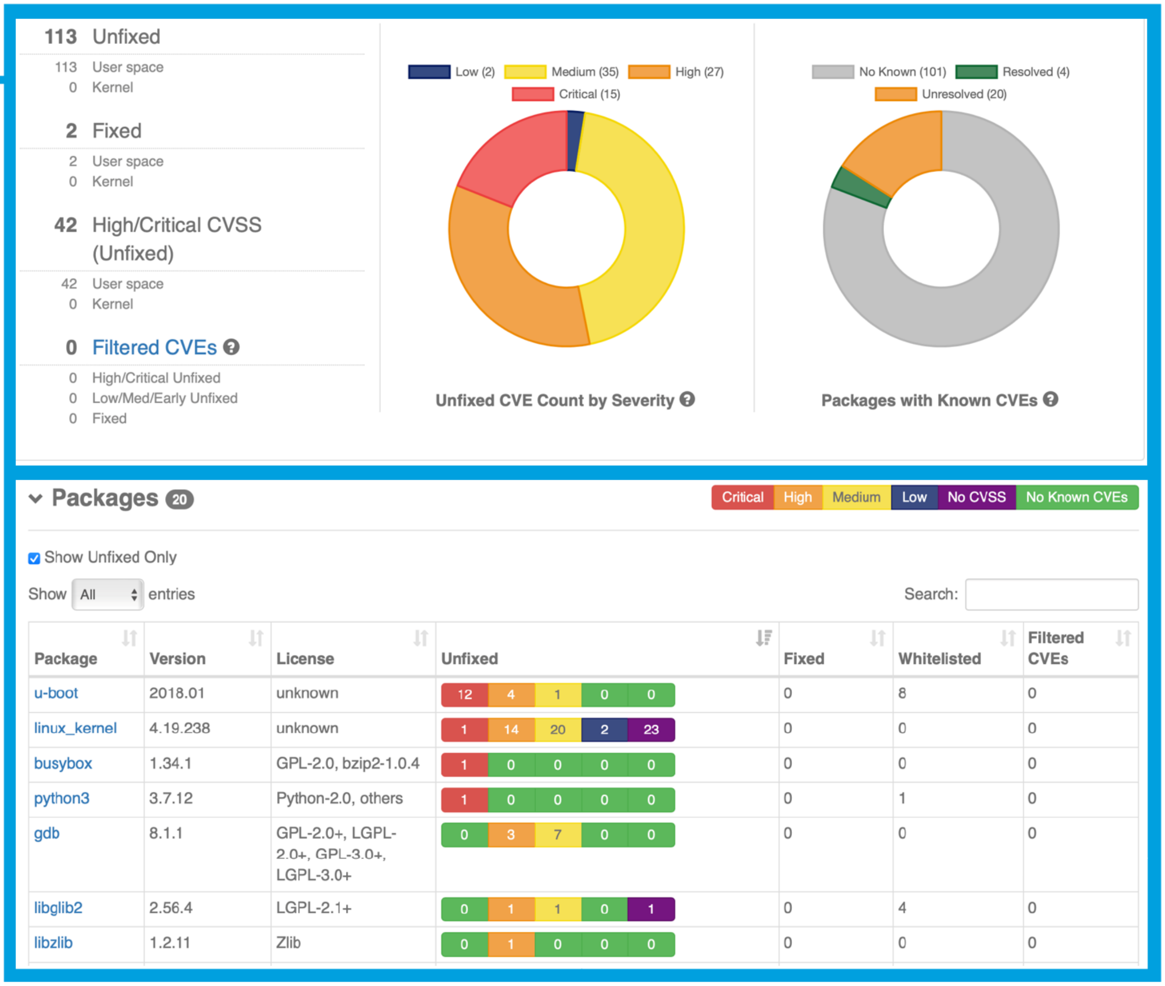
| **Summit Buildroot Linux BSP Releases** | 2022 | | | | 2023 | | | | 2024 | | | | 2025 | | | | 2026 | | | | 2027 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| Future Release | | | | | | | | | | | | | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ |
| Release 12 - LTS Kernel and LTS Buildroot | | | | | | | | | | 12 R1 | | 12 R2 | | 12 R3 | | 12 R4 | | Further Releases Summit Suite Only | | | | | | |
| Release 10 – 5.15 Kernel 2022.02 Buildroot | | 10 R1 | | 10 R2 | | 10 R3 | | 10 R4 | | Further Releases Summit Suite Only | | | | | | | | | | | | | | |


Software Security Life Cycle
QA Cycle
Release updated BSP
Release SW into the field
CVE Triage and Remediation
Software patches or new package version
VIGILES®
timesys
Select Hardware Platform
Use our BSP For Development, Finalize SBOM
CVE Monitoring and Reporting (Vigiles Prime)

# Industry-Leading CVE Monitoring and Reporting with Vigiles Prime

Vigiles Prime provides web-based, easy to digest CVE reports with detailed information for every vulnerability in each software package in your SBOM. It displays the CVSS score, fixed version, and links to patches for fixes. Reports are exportable and shareable, and email alerts can be configured to be sent daily, weekly, or monthly on newly discovered CVEs in your SBOM. If you're regularly creating updated SBOMs for your product, these can be automatically uploaded into Vigiles Prime from your continuous integration and build process via Vigiles Prime's APIs.

VIGILES
timesys
**CVE Monitoring and Reporting (Vigiles Prime)**



| | |
|---|---|
| **113** | **Unfixed** |
| 113 | User space |
| 0 | Kernel |
| **2** | **Fixed** |
| 2 | User space |
| 0 | Kernel |
| **42** | **High/Critical CVSS (Unfixed)** |
| 42 | User space |
| 0 | Kernel |
| **0** | **Filtered CVEs** |
| 0 | High/Critical Unfixed |
| 0 | Low/Med/Early Unfixed |
| 0 | Fixed |

**Packages** 20

☑ Show Unfixed Only

Show All entries

Search:

| Package | Version | License | Unfixed | Fixed | Whitelisted | Filtered CVEs |
|---|---|---|---|---|---|---|
| u-boot | 2018.01 | unknown | 12 4 1 0 0 | 0 | 8 | 0 |
| linux_kernel | 4.19.238 | unknown | 1 14 20 2 23 | 0 | 0 | 0 |
| busybox | 1.34.1 | GPL-2.0, bzip2-1.0.4 | 1 0 0 0 0 | 0 | 0 | 0 |
| python3 | 3.7.12 | Python-2.0, others | 1 0 0 0 0 | 0 | 1 | 0 |
| gdb | 8.1.1 | GPL-2.0+, LGPL-2.0+, GPL-3.0+, LGPL-3.0+ | 0 3 7 0 0 | 0 | 0 | 0 |
| libglib2 | 2.56.4 | LGPL-2.1+ | 0 1 1 0 1 | 0 | 4 | 0 |
| libzlib | 1.2.11 | Zlib | 0 1 0 0 0 | 0 | 0 | 0 |

# Ordering Information

| Part Number | Description |
|---|---|
| SAAS-SS-CVE-WB45 | One Year of Software Vulnerability Monitoring and Remediation for the WB45NBT |
| SAAS-SS-CVE-WB50 | One Year of Software Vulnerability Monitoring and Remediation for the WB50NBT |
| SAAS-SS-CVE-SOM60 | One Year of Software Vulnerability Monitoring and Remediation for the 60 Series SOM |
| SAAS-SS-CVE-IG60 | One Year of Software Vulnerability Monitoring and Remediation for the IG60 |

Interested in our Summit Suite?
Visit us at https://www.lairdconnect.com/iot-software/summit-suite