

# Timesys BSP Lifecycle Maintenance

Your BSP + Our Maintenance and Security Expertise = 60% Reduction in Maintenance Costs

Keeping your product line updated and in sync means high maintenance costs. There's the cost of having to manage multiple versions of Linux, for multiple generations of a product, and for multiple variants. And to keep your product secure, there's the on-going cost of being able to identify issues in all your production releases and respond rapidly and efficiently when vulnerabilities and patches affecting your BSPs are identified. With so much of your resources tied up in maintaining your BSP, it's difficult to focus on your value-add application, new feature development and next-generation product.

Timesys BSP Lifecycle Maintenance will:

- Keep your OSS BSP software components up to date
- Monitor security issues and patches for your BSP
- Patch, update and test your BSP

**Timesys BSP Lifecycle Maintenance significantly lowers the long-term maintenance costs associated with keeping your product line updated and secure — our customers have proven a 60% reduction in their costs.**

## Timesys BSP Lifecycle Maintenance Service enables you to do more with less

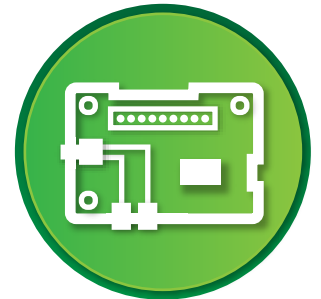
Long-term maintenance of a BSP/Linux software platform is a time-consuming effort that requires dedicated, often full-time engineers with expertise in Linux kernel development, build systems, software update implementation, and security vulnerability monitoring and patch management.

Rely on the expertise of the Timesys BSP maintenance team to:

- **Keep Your Product Line Updated, and In Sync** — The Timesys BSP maintenance team takes on the task of updating your BSP and keeps it in sync with latest releases (compilers, user space packages, major kernel and Yocto Project upgrades) as per your requirements. Along with updating your BSP, we also rebuild the SDK.
- **Stay Secure** — Our BSP Lifecycle Maintenance Service relieves your team of the burden of constant CVE monitoring and analyzing their impact by utilizing Timesys' Vigiles Security Software Composition Analysis (SCA) and mitigation tool. Our Maintenance service manages every step of the process for you, from vulnerability identification and assessment to patch integration. So your system is patched quicker, minimizing the chance of your product being exploited.
- **Receive Ready-to-Deploy Updates** — After integrating patches/updates, we validate the BSP using the Timesys driver testing framework. We provide you with the updated BSP along with test reports and documentation to help you with compliance.

## Timesys brings open source embedded software expertise to your BSP maintenance

When you engage with Timesys for BSP Lifecycle Maintenance, we maintain your BSP for you and keep it secure, in the most cost-efficient way possible. We've worked with hundreds of boards, on thousands of projects and with numerous build systems including: Yocto Project, Timesys Factory, Buildroot, PetaLinux, and LTIB. All of this experience has enabled us to streamline the process of Linux BSP development and maintenance.



*"We chose to partner with Timesys in the development of our new portfolio of medical devices to ensure that they stay secure throughout their lifecycle. Our customers globally face strict information security requirements combined with a heightened threat environment when deploying these devices within their enterprise. Our secure design methodology, partnership with Timesys, and operational policies allow our customers to be confident in choosing and deploying these devices in their healthcare practice."*

— Roshy J. Francis,  
Chief Technology Officer of  
Diagnostic Cardiology for GE  
Healthcare

## Timesys BSP Lifecycle Maintenance includes:

- Subscription to Vigiles Prime
  - Security & vulnerability notification and reporting tool for monitoring your software
- Monthly Security Notification reports
  - CVE report for user space, kernel, toolchain
- BSP update twice a year
  - Minor kernel version upgrade for security and bug fixes
  - User space security patching/package update
  - SDK (Development configuration and Production configuration)
  - Two releases per year on a mutually agreed upon timelines
- Functional driver test reports
  - Release notes & test reports
  - Hardware maintained in Timesys Remote Access Embedded Board Farm
- How-to-Use documentation
- Bidirectional Git – Upload/download BSP sources and changes
- One on-demand update for emergency security fixes

## Optional add-ons include:

- Kernel/drivers and U-Boot major version upgrades
- Yocto upgrade
- Custom BSP update cadence
- Additional on-demand update for emergency security fixes

Timesys BSP Lifecycle Maintenance includes CVE and test reports.

ST.No	CVE ID	Summary	Published Date	Modified Date	CVE Type	CVSS Score (V2 / V3)	Severity	Scope (Attack Vectors)	Affected Firmware Version
1	CVE-2017-14106	The <code>tip_disconnect</code> function in <code>netfilter4tcp.c</code> in the Linux kernel before 4.12 allows local users to cause a denial of service ( <code>_tip_select</code> without divide-by-zero error and system crash) by triggering a disconnect within a certain <code>tip_resmg</code> code path.	09/01/2017	09/26/2017	Denial Of Service	5.5	Medium	Local	Before 4.12
2	CVE-2017-14140	The <code>more_jpages</code> system call in <code>mm/migrate.c</code> in the Linux kernel before 4.12.6 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid process's double <code>ELF</code> .	09/05/2017	09/26/2017	Obtain Information	5.5	Medium	Local	Before 4.12.6
3	CVE-2017-12146	The driver <code>_override</code> implementation in <code>diversibase/platform.c</code> in the Linux kernel before 4.12.1 allows local users to gain privileges by leveraging a race condition between a read operation and a store operation that modifies different pointers.	09/08/2017	09/26/2017	Gain privileges	7	High	Local	Before 4.12.1
4	CVE-2017-00001	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3rc1 and up to and including 4.13.1 are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.	09/12/2017	09/27/2017	Execute Code/Arbitrary Code Execution	8.8	High	Adjacent	3.3rc1 and to and including 4.13.1
5	CVE-2012-12183	A security flaw was discovered in the <code>h80211_get_key_data()</code> function in <code>net/wireless/h80211.c</code> in the Linux kernel through 4.13.3. This function does not check whether the required attributes are present in a <code>h80211_key</code> request. This request can be issued by a user with the <code>CAP_NET_ADMIN</code> capability and may result in a NULL pointer dereference and system crash.	09/21/2017	09/22/2017	Not available	Not available	Not available	Not available	Through 4.13.3

Test Case	Description	Test Arguments	Status	Comment
<b>GSTREAMER</b>				
243	PIPELINE	/tmp/input.avi /tmp/output11 /tmp/input2.avi	PASS	
242		/tmp/input.avi /tmp/output11 /tmp/input2.avi	PASS	

To learn more about Timesys BSP Lifecycle Maintenance, email us at [sales@timesys.com](mailto:sales@timesys.com) or call us at **1.866.392.4897** (toll-free) or **+1.412.232.3250** to schedule a complimentary, no-obligation consultation.

**Disclaimer:** Security is an ongoing process and is not foolproof. Timesys' security offering provides assistance with minimizing known vulnerabilities based on known issues, but doesn't have any warranty.

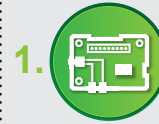


**Headquarters / North America Office:**  
 1905 Boulevard of the Allies,  
 Pittsburgh, PA 15219 UNITED STATES  
 1.866.392.4897  
 sales@timesys.com

**EMEA Office:**  
 ul. Palmowa 1A,  
 62-081 Chyby POLAND  
 +48.53.733.8080  
 emea@timesys.com

**APAC Office:**  
 3rd Floor, Jaag Homes, Achyutha Square,  
 No. 3, MTH Road, Villivakkam,  
 Chennai, Tamil Nadu – 600 049 INDIA  
 +91.0124.4299897  
 apac@timesys.com

## How It Works



### 1. Set Up Baseline

We set up a baseline that includes:

- Adding your custom board into the Timesys Board Farm Cloud
- Adding your BSP code into a private Git repo that only you and Timesys can access
- Running a driver test



### 2. Review Reports

We provide monthly vulnerability reports, and on a quarterly basis we jointly review them to determine what updates and patches you want us to apply.



### 3. Integrate Patches/Updates

We integrate security patches / package updates for your BSP as per the quarterly review.



### 4. Validate BSP

After integrating patches/ updates, we validate the BSP by comparing the driver tests against the baseline.



### 5. Deliver Updated BSP & Reports

We deliver updated BSP and validation reports for comparison with the previous report.