

# TRST Stay Secure: Timesys Vigiles – Real-time Monitoring for More Secure Products

Security notification tailored to your software platform + Patch/upgrade = Peace of mind

Maintaining your device’s established security posture is no easy task. With the increasing rate of security vulnerabilities and the unpredictability of discoveries, keeping up with this manually is time-consuming, and it’s just not feasible.

Every day, you need to keep up with newly issued CVEs by monitoring security databases and mailing lists and identifying CVEs which are relevant for the version of each software component included in your system. Once relevant issues are identified, you’re still tasked with the process of finding and applying security updates and patches to your software.



Timesys Vigiles will:

- Notify you when known security issues (CVEs) that are specific to your product are found
- Provide you with the status (fixed or unfixed) of the vulnerabilities
- Provide you with links to the fixes
- Allow you to selectively apply updates and patches to your software

**Vulnerabilities by Year:  
Hackers Are Forcing New  
Maintenance Processes  
to Stay Secure**

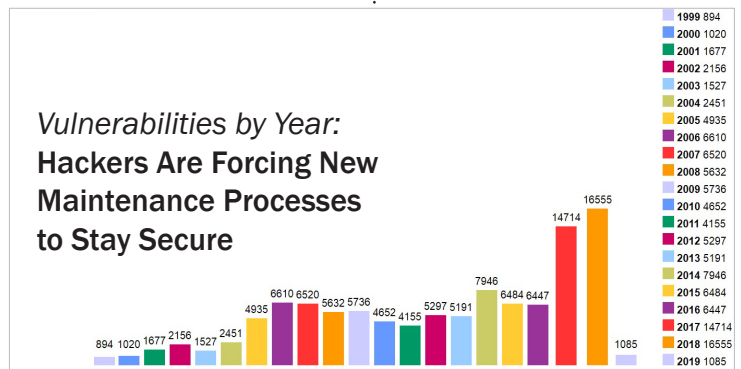


Image source: cvedetails.com

**Timesys Vigiles automated security vulnerability monitoring and patch notification helps to significantly reduce the time and costs associated with maintaining software security — our customers have proven ROI.**

## Timesys Vigiles enables you to more efficiently manage and maintain your device’s security posture

Rely on Timesys Vigiles automated security vulnerability and patch notification to help you:

- **Eliminate the time spent monitoring vulnerabilities** — Our service relieves your team of the burden of constant CVE monitoring and analyzing their impact by utilizing Timesys TRST technology. With Timesys Vigiles, you receive on-demand notification of vulnerabilities relevant to only your software.
- **Remain in control of security fixes** — You receive minimum kernel version information and a link to the corresponding patch. You can selectively apply patches ... so you decide what gets updated.
- **Stay Secure** — Our service helps you minimize the chance of your software being exploited. Because Vigiles makes it easier for you to manage vulnerability identification, assessment and patch/update integration, you can respond to CVEs rapidly and efficiently.

## Timesys brings open source embedded software expertise to helping you stay secure

When you subscribe to Timesys Vigiles for your vulnerability monitoring and patch notification, we help you keep your embedded Linux based product 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 entire process of monitoring, analyzing and responding to vulnerabilities for better embedded Linux security.

*“Security is at the forefront of today’s IoT issues as the discovery of new vulnerabilities and the rate of attacks continue to escalate. Improving security is becoming especially critical for IoT and IIoT devices because of the rapid expansion of deployments combined with the rise in botnet, bricking and other attacks against these smart devices. Timesys is bringing to market a timely solution, designed to make these devices more secure and maintain that improved security posture into the future.”*

– Roy Murdock, VDC Research

## Timesys Vigiles options:

Activate Vigiles Basic and get Prime FREE for 30 days

Features	Vigiles Basic	Vigiles Plus	Vigiles Prime
Duration/term	Free for 1 year	Yearly subscription	Yearly subscription
BSP security vulnerability rating reports	Summary	Detailed	Detailed
CVEs affecting your software components	Detailed	Detailed	Detailed
Push notifications of vulnerabilities	Summary	Detailed	Detailed
Track multiple component lists (build system independent)	Limited to 1	Unlimited per product family	Unlimited per product family
Compare accuracy with open source tools	Summary	Summary	Summary
Compare kernel false positives with NVD database	Summary	Summary	Summary
View overall counts of CVEs by severity and status	Detailed	Detailed	Detailed
CVE mitigation collaboration tools		✓	✓
Continuously track specific issues and CVE status changes		✓	✓
On-demand/pull notifications via command-line and Web	Summary	✓	✓
View fixed and unfixed CVEs for Yocto	✓	✓	✓
Whitelist already reviewed CVEs to streamline reviews		✓	✓
Categorizes by kernel, libraries, CPU and whitelisted CVEs	✓	✓	✓
Filter reports by severity (CVSS) score		✓	✓
Download reports in different formats		✓	✓
Link to the patch for Linux kernel CVEs			✓
Minimum kernel version with a fix for a kernel CVE			✓
Filter reports based on kernel configuration (experimental)			✓
Minimum package version with a fix for userspace library/packages (experimental)			✓

## How It Works

### 1. Discover and Identify

The Timesys TRST Team utilizes a Timesys-built Common Vulnerabilities and Exposures (CVE) manager to gather information from nvd.nist.gov and security mailing lists and identify security issues relevant to the code in the Timesys source code repository.

### 2. Analyze

The Timesys TRST Team then analyzes the state of the vulnerability (known vulnerability with available patch or update vs. known vulnerability with no fix available).

### 3. Get Notification

To determine if any security issues are known to affect your project in your Yocto Project or Timesys Factory desktop development environment – or any other build environment or application using open source components – you can pull notification by running a checkcves command. Or you can upload your software component list to your security project in the LinuxLink portal and get push notification for each.

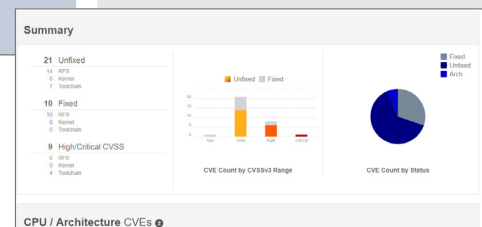
### 4. Triage

Triage a CVE by collaborating with other members of your team. You can also ignore a CVE by adding it to the whitelist.

### 5. Patch

For kernel CVEs, you are notified of the minimum kernel version and provided with the link to the associated patch for each. You determine which CVEs you want to fix and selectively apply the patches.

For CVEs associated with a user space package or library, you are notified of the minimum fixed version for each. You determine which CVEs you want to fix and selectively upgrade to required version.



Online graphical reports enable a quick visual assessment of the state of vulnerabilities relevant to your software.

To learn more about Timesys Vigiles, 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