Stay Secure: Timesys Security Vulnerability and Patch Notification Service

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. And once relevant issues are identified, you're still tasked with the process of finding and applying security updates and patches to your software.

Timesys Security Vulnerability Monitoring and Notification 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

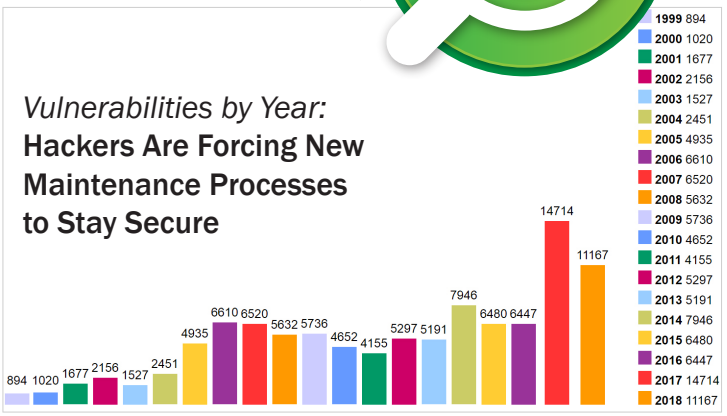


Image source: cvedetails.com

Timesys' automated Security Vulnerability Monitoring and Notification service helps to significantly reduce the time and costs associated with maintaining software security — our customers have proven ROI.

Timesys Security Vulnerability Monitoring and Notification service enables you to more efficiently manage and maintain your device's security posture

Rely on Timesys Security Vulnerability and Patch Notification service 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 (Threat Resistance Security Technology). With Timesys Security Vulnerability Notification, you receive on-demand notification of vulnerabilities relevant to only your software.
- **Remain in control of security fixes** — With Timesys Patch Notification service, you can add or update the meta-timesys-security layer, where the Timesys TRST team has added available updates and patches. And 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 our Security Vulnerability and Patch Notification service makes it easier for you to manage vulnerability identification, assessment and patch/update integration, you can respond to CVEs rapidly and efficiently.

"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."

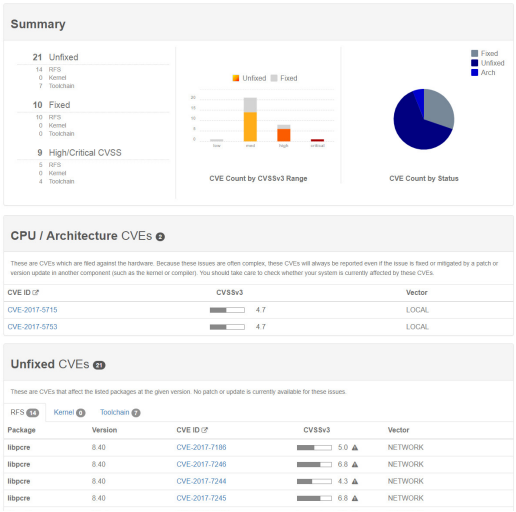
– Roy Murdock, VDC Research

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

When you subscribe to Timesys Security Vulnerability and Patch Notification Service, 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.

Timesys Security Vulnerability and Patch Notification features:

- Pull notifications for current vulnerabilities via command-line and Web
- Minimized false results
- Ability to subscribe to push notification via Web portal
- Tracking of the number of affected issues and CVE status changes for each build
- Reporting of fixed/patched CVEs within your software BOM
- Ability to create and use whitelists, enabling you to skip already reviewed CVEs
- Separate patch layer for easy integration
- Ability to subscribe to multiple software configurations
- Ability to view online reports with charts of overall counts, breakdown of CVEs by severity and status
- Reports that are categorized — kernel, libraries, CPU and whitelists
- Ability to download reports in various formats
- Support for Yocto Project development
- Very responsive, quick scan times



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

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. Update and Patch

The Timesys TRST Team adds available security updates and patches to the code in the Timesys source code repository, including meta-timesys-security.

4. Get Notification

To determine if any security issues are known to affect your project in Timesys' Yocto Project Café or Factory desktop development environment, you can pull notification by running a checkcves command.

You have the option to store your workorder(s) or manifest(s) in Timesys' web development environment and get push notification for each.

5. Get Patch

You add or update the meta-timesys-security layer. (meta-timesys-security is where the TRST team continually adds available security updates and patches for the current and previous two Yocto versions.)

6. ApplyPatch

You determine which CVEs you want to fix and configure your recipes (.bbappend) to selectively include the patches.

To learn more about Timesys Security Vulnerability and Patch Notification service, email us at **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.*

timesys®

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, Time Square Building,
Shushant Marg, Sushant Lok I, Sector 43,
Gurugram, Haryana – 122009 INDIA
+91.0124.4299897
apac@timesys.com

Copyright © 2018 Timesys Corporation. All Rights Reserved.

Timesys and the Timesys logo are registered trademarks of Timesys Corporation. Linux is a registered trademark of Linus Torvalds in the United States and other countries. All other company and product names mentioned and marks and logos used are trademarks and/or registered trademarks of their respective owners.