ADVANTECH
Enabling an Intelligent Planet

timesys

More Secure, Compliant Medical Devices using Advantech Platforms with Timesys Security Solutions

Get to market faster with streamlined cybersecurity compliance assistance

A successful cybersecurity breach can put patients at risk, compromise healthcare outcomes and violate privacy laws. But medical device security compliance is not only critical to patient safety — it is required by the FDA, among other associations, to get your product into the market.

Boost compliance with medical device security standards and regulations

Timesys tools and services can assist you in meeting compliance requirements in the following areas:

- FDA Guidance (FDA-2018-D-3443) for Premarket submissions, such as 510(k)
- FDA Guidance (FDA-2015-D-5105) for Postmarket Management of Cybersecurity
- NEMA Requirements for Manufacturer Disclosure Statement for Medical Device Security
- IEC 62304: Software Life Cycle Processes

With more than 20 years of experience in embedded systems, Timesys is an industry leader in open source software security, offering complete end-to-end device security solutions.
Timesys provides compliance assistance by offering:

- **VigiShield Secure by Design service** — implement best-in-class security features utilizing hardware and software (e.g.: secure boot, encrypted storage, trusted execution environments, etc.)
- **Vigiles vulnerability management tool** — Software Composition Analysis (SCA) and Common Vulnerabilities and Exposures (CVE) monitoring and remediation product optimized for embedded Linux
- **Linux OS and BSP Maintenance** — subscription service that provides long-term security updates and maintenance for Linux OS and BSPs

Generate an accurate Software Bill of Materials (SBOM) with Vigiles

An SBOM is essential to understanding what you're shipping, and to maintaining the security of your device. Timesys has created plugins for various build systems including Yocto, Buildroot, OpenWrt, and Timesys Factory to easily and accurately generate an SBOM.

Try out Vigiles Prime free for 30 days to generate your SBOM, and see your vulnerability report: www.timesys.com/register-prime/

Timesys Security Solutions assist you in meeting industry requirements for device security by:

- Implementing device hardening, secure boot, and chain of trust
- Encrypting storage media and protecting keys/passwords
- Customizing a trusted OS and applications in the Trusted Execution Environment (TEE)
- Integrating secure remote Over-the-Air (OTA) updates
- Creating a Software Bill of Materials (SBOM)
- Monitoring, triaging, and remediating vulnerability-related threats
- Providing security updates of Linux OS and Software of Unknown Provenance (SOUP)
- Providing documentation of security-related updates

Timesys Security Solutions provide:

Software security feature implementation and enablement

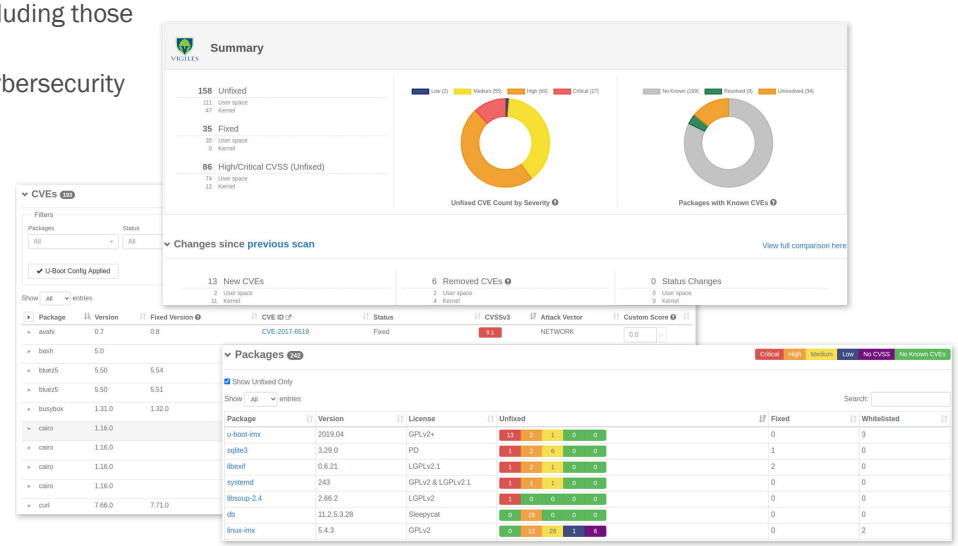
Vulnerability monitoring and remediation

Long-term software updates and security maintenance

These solutions help to boost compliance with the following medical device security standards and regulations:

- **FDA Guidance (FDA-2018-D-3443) for Premarket submissions, such as 510(k):**
  - Cybersecurity measures during the design and development of medical devices
  - Identification of assets, threats, and vulnerabilities
  - Ensure trusted content by maintaining code, data, and execution integrity
  - Maintain confidentiality of data
- **FDA Guidance (FDA-2015-D-5105) for Postmarket Management of Cybersecurity:**
  - Monitoring cybersecurity information sources
  - Monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle
  - Understanding, assessing and detecting presence and impact of a vulnerability
  - Validation for software updates and patches that are used to remediate vulnerabilities, including those related to off-the-shelf software
  - Deploying mitigations that address cybersecurity risk early and prior to exploitation
- **NEMA Requirements for Manufacturer Disclosure Statement for Medical Device Security:**
  - Generate a Software Bill of Materials (SBOM) and provide a process to update it as specified in MDS2
  - Implement device hardening, security updates, remote updates, security of third-party components and other cybersecurity controls specified in MDS2
- **IEC 62304: Software Life Cycle Processes**
  - Processes for managing medical device software risks, maintenance and trouble resolution
  - Identify and manage cybersecurity risks for Software of Unknown Provenance (SOUP)

To learn more about how our security solutions can help with compliance to get your product to market faster, visit www.timesys.com/security/.



The Vigiles CVE dashboard enables you to see the highly accurate CVE list that applies to your software bill of materials (SBOM)/manifest. You can filter vulnerabilities for your product, triage the results, and start applying the remediation needed for the CVEs that you prioritize.

Sign up for a free 30-minute security consultation to see which Timesys products and services will help you meet your compliance requirements at **www.timesys.com/schedule-consultation-advantech/.**

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

Rev. 03-20220114A