Solution Note

timesys

VIGILES™

Timesys Vigiles: Security Optimized for Embedded System Medical Devices

- Industry's only SCA tools optimized for embedded open source, including Yocto, Buildroot, and Timesys Factory Linux, and open source package monitoring
- On-demand vulnerability monitoring and simple security maintenance for more secure medical device products
- Boosts security standard compliance: IEC 62304, FDA Premarket and Postmarket Security Guidance
- Supports 'Secure by Design' development, faster time-to-market for secure products that stay secure throughout lifecycle
- Filter, triage, investigate and mitigate vulnerabilities based on your exact Software Bill of Materials (SBOM)
- Most accurate vulnerability tracking for embedded systems for fewer false positives
- Advance notice on vulnerabilities before general industry notifications
- Get started now for free

Medical device security is critical. A successful cybersecurity attack can put patients at risk, compromise health care outcomes and violate privacy laws.

With more than 20 years of embedded system development and maintenance experience, Timesys has captured the industry's best practices for embedded system security. Our tools and services enable medical device manufacturers to streamline development and maintenance of secure products.

Timesys Vigiles is the industry's only vulnerability tracking and security maintenance service optimized for embedded systems. Your products will be more secure at release and stay secure throughout the lifecycle.

Faster Time-to-Market with More Secure Medical Products Using Superior Vulnerability Data

Gone are the days when you could freeze your software at release and never touch it again. Device connectivity is now the norm, and hundreds of new vulnerabilities are uncovered every week, putting devices and customers at risk of compromise.

Vigiles continuously monitors multiple vulnerability feeds including the National Vulnerability Database (NVD) for better coverage across all vulnerabilities affecting your products and automatically sifts through the noise to flag only those issues that affect your products. Our curated service provides a 40% accuracy improvement over NVD data alone. Now your team wastes less time chasing "Vulnerability Ghosts" and false positives.

Vigiles also features expedited notification of newly reported vulnerabilities before they appear in the NVD. You have a critical head start in addressing vulnerabilities before they hit the news.

GE Healthcare: *"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

Now your software incorporates the latest, most secure versions of Linux and other open source software components, including updates and patches. Linux kernel configuration and U-Boot configuration tracking filters out vulnerabilities that affect features not used in your product. On average this reduces the vulnerability triage burden by a factor of 4X.

Timesys also offers proven, expert guidance on Secure by Design best practices including secure boot and encrypted data storage. Even if your medical device is not handling patient data directly, Timesys solutions cut the chance that a breach would put other systems at risk. Our solutions help your customers avoid privacy breaches of Protected Health Information (PHI) of the sort protected under HIPAA and other regulations.

(Continued)

Secure Products that Stay Secure

Timesys provids solutions to the Top 30 medical device makers, helping them build FDA Class I, II, and III medical devices.

- **Imaging:** CT/PET/X-Ray Instrumentation
- Therapeutics: Infusion Pumps, Surgery Devices, etc.
- **Biotech and Life Sciences:** DNA sequencing, Genetic Analysis
- **Diagnostics:** Cardiology, Hematology, Immunoassay, Analyzers

Boost Compliance with FDA Guidance & Standards

IEC 62304 requires medical device makers to ensure security of third-party software used in medical devices, such as Linux and open source packages. FDA medical device security guidance mirrors these requirements. Vigiles provides simple-to-use tools to streamline security maintenance and boost compliance with these security requirements:

- Security integration with design tools and workflows, including Yocto
- Accurate, continuous vulnerability reporting based on your actual documented system configurations and SBOM
- Streamlined security issue investigation, triage, and mitigation
- Timely notification of third-party software updates and patches correlated to identified vulnerabilities
- Reports enabling you to document security maintenance, aligning with FDA premarket guidance for products in development and postmarket guidance for released products

Get Started Now

Vigiles reduces cycles spent analyzing and addressing vulnerabilities by 90 percent or more. **The service is available in a completely free version** that enables you to start tracking and filtering vulnerabilities right now.

Learn more at: https://www.timesys.com/security/vigiles-vulnerability-monitoring-patch-notification/

Working with Timesys: Key Capabilities and Benefits

Secure by Design

- Software and BSP development respecting medical device market security standards and guidance (vulnerability analysis, review of the development process, mitigation workflows, documented security processes, etc.)
- Embedded System Devices, Internet of Things Devices, Air-Gapped Systems
- Secure connectivity between devices (WiFi, BT, RFID, NFC, etc.)
- Secure Over-the-Air (OTA) update processes
- Secure, interconnected, machine-to-machine (M2M) embedded systems with real-time performance
- Remote access and multi-dimension user interfaces
- Accurate visibility of vulnerabilities affecting your SBOM
- Cross-platform, custom, embedded and mobile applications integration (native technologies in C/C ++, Qt, HTML5, Node.js, Django, Java, Microsoft.NET)
- BSP Hardening, secure boot, encryption
- Full BSP integration and optimization, hardware/software compatibility, and middleware validation testing

Stay Secure

- Continuous, ongoing tracking of vulnerability notifications, patches and upgrades specific to your SBOM
- Auto generation, uploading, editing and management of your SBOM
- Curated vulnerability monitoring cutting false positives by 40 percent
- Early vulnerability notification up to 4 weeks before NVD notifications
- Support for reporting CPU/SoC vulnerabilities
- Team collaboration and communication for rapid triage and mitigation of vulnerabilities
- Powerful “comparison” capability for quick and easy visibility
- Full BSP lifecycle maintenance service available for turnkey outsourcing of monitoring, patching and updates

Contact Timesys today for a no-obligation consultation on medical device security best practices. Email us at **sales@timesys.com** or call us at **1.866.392.4897** (toll-free) or **+1.412.232.3250**.

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. 02-20200317A