Vigiles Frequently Asked Questions (FAQs)

Q&A Document
May 17, 2021

Product Features

Technology

Glossary of Terms

FAQs: Product Features

1. What is the difference between Vigiles Free, Plus and Prime?

Vigiles Free is the free, basic version and provides you with vulnerability monitoring and summary reports for 1 of your product manifests (software inventory that you load in Vigiles).

Vigiles Plus provides vulnerability monitoring and more detailed reports for an unlimited number of product manifests in a single product family, along with collaboration and communication tools to enable your team to analyze and work on mitigation for vulnerabilities.

Vigiles Prime provides all vulnerability identification and collaboration tools and expands the security management scope to include our unique Patch Notification & Management features, identifying patches and minimum versions to secure the software components that are identified in your manifests.

2. How does Patch Notification & Management in Vigiles Prime help with vulnerability management?

By identifying patches and minimum fixed versions, the patch management features of Vigiles Prime slash the amount of time your team spends on investigating identified vulnerabilities and exploring the mitigation steps to fix them.

Without Vigiles Prime patch management, your triage and mitigation activities will include identifying each component supplier and researching which version of a component has an available fix for a given vulnerability, if one is even available.

In contrast, Vigiles Prime patch management will automatically notify you of a patch associated with a given vulnerability for your specific components. Vigiles Prime will give you a direct link to the download for the patch. Further, Vigiles Prime will provide you with details on the minimum versions of libraries or packages and kernels that address the identified vulnerability.

Our analysis shows that Vigiles can cut your vulnerability identification and mitigation process cycles by 90 percent when compared with manual detection, investigation, and mitigation.

3. What are Triage Collaboration and Mitigation Tools in Plus and Prime?

These tools enable you and your team members to annotate, comment on, whitelist and otherwise collaborate on the vulnerabilities identified in your loaded product manifests. These communications tools are the foundation of highly efficient security vulnerability management workflows and risk mitigation processes.

For example, a team assigned to review a set of vulnerabilities might assign some team members to conduct impact analysis. Those team members can communicate quickly and easily about their evaluation of the security risks posed by specific vulnerabilities.

Other members may focus on high severity vulnerabilities to investigate expedited mitigation options, sharing their findings to weigh options and accelerate the response and fix.

Throughout these processes, some vulnerabilities may be whitelisted, which means they are tagged as acknowledged and in process or fixed. That way they do not clutter up the broader evaluation of inbound vulnerabilities or the mitigation workflows.

Along with flexible filtering, dashboarding, and reporting features, these collaboration tools can significantly cut the time your team spends on understanding the impact of a vulnerability and fixing it.

4. **How do I upgrade to Plus or Prime?**

   Just click here to upgrade at any time.

5. **Is Vigiles open source?**

   Vigiles is divided into two parts.

   The first part of Vigiles collects the software manifest from a Yocto project and is licensed under MIT license with Timesys copyrights (see: https://github.com/TimesysGit/meta-timesys/tree/zeus).

   The second part consists of the Vigiles scanner, backend database and user interface. This part of Vigiles is a Timesys proprietary product.

6. **Does Vigiles only support Yocto or does it support other build systems? Are custom Linux kernel, crosstools and bootloaders also supported?**

   Vigiles supports a number of build systems, including: Buildroot, Yocto Project and Timesys Factory. And Vigiles can be used with other build systems as well.

   Using the Vigiles UI, you can upload software manifests from any of the three build systems mentioned. In addition, Vigiles supports .csv format, so you can generate a software manifest from any other build system and format it as a .csv spreadsheet that you can upload. We provide guidance on creating a Vigiles .csv manifest here: https://linuxlink.timesys.com/docs/wiki/engineering/VigilesCSV (Vigiles account required to access).

   You can also create your software manifest from scratch entirely online using the Vigiles “Create Manifest” UI.

7. **Can Vigiles be used with any BSP or processor?**

   As mentioned above, Vigiles is integrated with different build systems. As long as your build system or manual SBOM is used, it can track vulnerabilities with one caveat — Vigiles tracks processor vulnerabilities. So, if your processor or architecture has vulnerabilities tracked by NVD, Vigiles will track it.

8. **Currently, we use Linux kernel 4.9 in our project. Can it be scanned using Vigiles or does the kernel need to be a newer version?**

   Yes, projects using Linux kernel 4.9 can be scanned for vulnerabilities using Vigiles. And projects using older versions of the Linux kernel can be scanned as well.

With older kernel versions, you should expect to see more vulnerabilities in the Vigiles report. In general, we recommend that our customers use a recent Long Term Support (LTS) version of the Linux kernel. Because security fixes get backported by LTS kernel maintainers, using a recent LTS version of the Linux kernel will allow you to leverage those backports in your BSP/product.

9. What is a product manifest?

A product manifest is the inventory of your product's software components and the versions in your design, loaded into Vigiles for security monitoring.

10. Do I need to manually load my product manifest each time a report is generated?

Vigiles does not require you to upload the product manifest each time it is run. In a typical Yocto build environment, the Vigiles Yocto layer will extract the manifest from your source code.

11. How are Vigiles results presented? Are the reports exportable (json/xml) for integration into company-wide issue trackers?

Yes. The Vigiles results can be exported. You can export them as a spreadsheet or a PDF, so the results can be easily integrated into your own issue tracker.

In the upcoming Vigiles release, you will also have the ability to get reports via JSON directly in your build system. This will provide further integration into your company-wide issue tracker.

12. Is there a limit to the number of the projects you can have in Vigiles?

No. For a given CPU, there is no limit to the number of projects you and your team can setup in Vigiles.

13. How is Vigiles different than other vulnerability scanners including Black Duck?

Vigiles is best suited for embedded. Specifically, Vigiles:

- Tracks CVEs already fixed in Yocto/Buildroot, letting you/your team focus on vulnerabilities that need to be fixed.
- Enables up to 4x reduction in CVE review with kernel and U-Boot configuration-based filtering.
- Provides superior vulnerability reporting with fewer false positives.
- Provides links to patches and commits, reducing time to needed address/mitigate vulnerabilities.
- Features an advanced filtering capability, helping you/your team to prioritize and focus on only the vulnerabilities that matter.

In addition, Vigiles customers have access to the Timesys TRST Security team for help with any CVE questions as well as access to a Managed BSP Maintenance Service option for those who do not want to fix the vulnerabilities themselves.

14. Does Vigiles support Android security patches?

Vigiles is not fully enabled for Android yet. However, you can use Vigiles and BSP Maintenance to monitor CVEs and fixes, and for help with triaging the Linux portion of Android.

For the Android Open Source Project components from Google, use the security tracking bulletin from Google (https://source.android.com/security/bulletin).

15. **Do Vigiles and Linux Test Project (LTP) overlap?**

    The two solutions do not overlap, but can be used together.

    Vigiles monitors vulnerabilities for the entire Linux BSP including the Linux kernel, bootloader and userspace packages, and LTP helps with verifying/testing Linux feature functionality. Therefore, you can use Vigiles to identify CVEs and available fixes, and then once you and your team go through triaging and fix implementation, you can run LTP to verify Linux functionality.

16. **Is it possible to run Vigiles on a device not connected to the Internet?**

    First, it's important to note that Vigiles does not interact with the target device.

    Vigiles works by extracting package/version information from the build system Yocto/Buildroot) or by the user generating/uploading a Software BOM CSV file to Vigiles. Vigiles then compares the list of packages/versions against a Timesys-curated vulnerability database and generates a web report accessible only by the end user and/or user's team.

    Currently, Vigiles is a hosted/cloud only solution. We do provide an on-premises version of Vigiles that can be on your network without internet access. However, we do plan to provide an on-premises version later this year.

17. **Is there way to use Vigiles with "Layerscape SDK" build process? Is there a way to use Vigiles with Layerscape BSP (Ubuntu-based)? Or should we generate a manifest from Ubuntu ourselves?**

    Currently, there is no direct support to extract the manifest from "Layerscape SDK" flex-builder, however, we are investigating adding support for Layerscape SDK in a future release of Vigiles to enable seamless integration.

    At this time, you can still use Vigiles with the Layerscape SDK. You can manually create a CSV file and/or use the Vigiles UI to create a manifest containing all the NXP packages and then upload it to Vigiles to generate a vulnerability report. If you need help, we can either assist you in creating the CSV file, or we can create it for you.

    Currently, for Layerscape Ubuntu-based BSPs, you can use Vigiles to monitor vulnerabilities for NXP packages. For Ubuntu userland packages, use Ubuntu security bulletin for tracking user space CVEs: https://people.canonical.com/~ubuntu-security/cve/universe.html

FAQs: Technology

1. **What is Vigiles?**

    Vigiles tracks Common Vulnerabilities and Exposures (CVEs), providing end-to-end vulnerability management, while improving on the CVE data publicly available from the National Vulnerability Database (NVD).

2. **How does it work? How does Vigiles determine which CVEs to report?**

    Vigiles pulls CVE information from National Vulnerability Database (NVD) every 24 hours.

For a particular CVE, there is a unique name for the specific software or hardware that is affected. This scheme is called Common Platform Enumeration (CPE), and it's used for mapping a CVE to a product name and version. Most commercial and open source tools use CPE.

If this hardware or software CPE appears in a client's Software Bill of Materials (SBOM), then Vigiles pulls the data for the corresponding CVEs. The SBOM is automatically generated for Yocto and Buildroot.

3. **Of the approximate 350 new CVEs announced each week, is this just the number of CVEs reported against the Linux kernel mainline?**

   The approximate number of 350 vulnerabilities reported each week refers to all vulnerabilities reported in CVE tracking databases for all software.

   On average, you should expect that approximately 10 CVEs/month will directly apply to your embedded Linux product. And many of these issues will indeed be reported for the Linux kernel itself.

4. **Can you get false positives?**

   Tools relying on CPE data from NVD, like Vigiles, are still prone to missed CVEs, false positives (reported CVE is not applicable to the package/version), and reporting delays.

   This can be due to CPE data quality issues (like incorrect product names or version information), incorrect SBOM information (name/version number), or delays in a CVE being published in the NVD.

   Timesys takes a number of steps to improve coverage and reduce false positives; see the next question and answer for further details.

5. **How does Vigiles filter out false positives?**

   Filtering out false positives begins with the Timesys TRST Security Team. The team uses in-house developed automation and some manual work to mark CVEs correctly in our in-house curated CVE database. This work, which involves fixing some of the issues typically encountered, such as version issues, LTS kernel minor release info, etc., enables us to host a curated CVE database that contains highly accurate CVE info.

   Then, Vigiles relies on our curated CVE database during the scanning process. In addition, Vigiles takes into account any filters you may applied such as the Linux kernel configuration and U-Boot configuration filters, along with factoring in any CVE patches already applied, resulting in a highly accurate security vulnerability report.

6. **How does Vigiles improve upon info from the National Vulnerability Database (NVD)?**

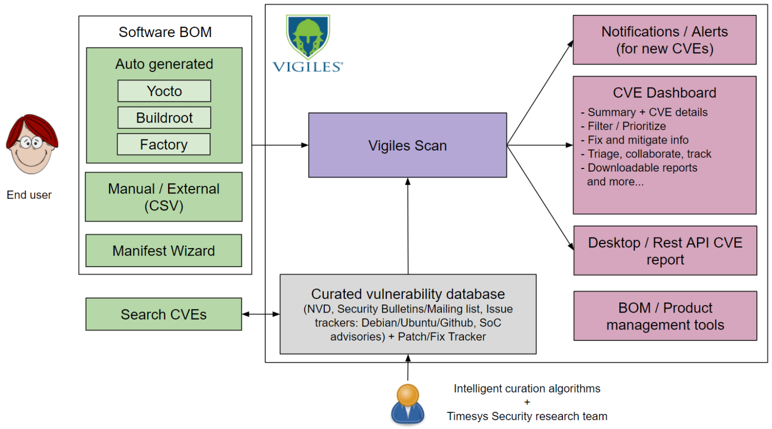
   Vigiles provides up to 40% accuracy improvement over the NVD with Timesys' curated CVE/CPE database.

   Timesys' security team has error detection mechanisms in place via our BSP Maintenance service, customer feedback, and upstream Yocto patch submissions. Using this info, the security team **manually analyzes** incorrect CVEs and updates it in our systems. We also cross-verify our database with Upstream mailing list, issue trackers, security bulletins, Debian/Ubuntu/RedHat security trackers, SoC vendor advisories.

   Additionally, we've created **intelligent curation algorithms** for the Linux kernel and u-boot that run on a nightly basis. We automatically update our curated database with fix commit and backports using git.

Finally, we minimize reporting delays. By augmenting our database with information from multiple feeds, we can notify our customers of CVEs not yet reported by the NVD — sometimes up to four weeks earlier!

Vigiles high-level architecture overview


Software BOM
Auto generated
Yocto
Buildroot
Factory
Manual / External (CSV)
Manifest Wizard
End user
Search CVEs
VIGILES
Vigiles Scan
Notifications / Alerts (for new CVEs)
CVE Dashboard
- Summary + CVE details
- Filter / Prioritize
- Fix and mitigate info
- Triage, collaborate, track
- Downloadable reports and more...
Desktop / Rest API CVE report
BOM / Product management tools
Curated vulnerability database
(NVD, Security Bulletins/Mailing list, Issue trackers: Debian/Ubuntu/Github, SoC advisories) + Patch/Fix Tracker
Intelligent curation algorithms
+
Timesys Security research team

7. **Does Vigiles have a way to catch errors like typos or missing mappings?**

   If a package in the SBOM is not found in our database, we alert the user in the CVE report page. The customer can fix the package name or map it to our database using the override mechanism. The Timesys security team also periodically reviews and adds missing mappings. And finally, it allows users to include/exclude packages from auto-generated SBOMs, and override mapping.

   However, Timesys cannot guarantee that Vigiles is entirely free from errors, defects, or bugs, currently known or unknown.

8. **Can Vigiles be used to report vulnerabilities in userspace applications?**

   Vigiles tracks vulnerabilities for all software layers in a Linux BSP. This includes the bootloader, Linux kernel, drivers, userspace packages, and applications.

   Vigiles does not scan your BSP source code for code injections. Vigiles reports on the version of individual software packages you are using in your BSP and a list of patches that are applied on top.

   Therefore, if CVEs are reported against application software you've used, Vigiles will be able to provide you with information. However, if you are using an in-house developed proprietary application for which CVEs are not reported, Vigiles will not be able to provide any vulnerability information.

9. **If we have made custom changes in the kernel driver, would Vigiles be able to report on related vulnerabilities?**

   Vigiles does not track custom changes to software at a source code level.

   If you modify the driver before applying a CVE patch, you will have to adjust the CVE patch to apply on top of your changes. Therefore, it is recommended to first apply a CVE patch and then make customizations. This would possibly require adjustments to your customization patch.

10. **What information is collected when I upload my product manifest for security monitoring?**

    Timesys Vigiles only collects package/recipe names, version, patches applied (if any), and build system version information. This information will only be shared with members of your team.

    Timesys Vigiles does not require you to upload your product source code.

11. **What does Timesys do with the information in my confidential product software manifest?**

    We currently don’t do anything with the customer information uploaded to Vigiles. Your product manifest(s) will remain in your Vigiles account for as long as you need.

    When no longer needed, you can delete the information you’ve uploaded yourself or ask us to delete it for you.

12. **What security measures has Timesys implemented to ensure my product software manifest does not get shared with other Vigiles users?**

    By default, all CVE links are private and are not accessible to other users based on login authentication.

13. **What assurances can Timesys provide that my product software manifest information will not be hacked or otherwise leaked from Vigiles?**

    Timesys stores all manifest information in an encrypted disk.

14. **How does Vigiles handle third-party source code that is included, but not shown in Yocto recipes? For example, QtWebEngine has Chromium source code included and hence is subject to the same CVEs as Chromium, with a number of proprietary patches. Will Vigiles report on these CVEs when including QtWebEngine?**

    If the Chromium CVEs are also marked for QtWebEngine, they will show up in the Vigiles report for the Qt package that contains QtWebEngine module. If a CVE is reported against Chromium but is not marked as applicable to QtWebEngine, Vigiles will not show it in the report.

    Applicability of a CVE reported on one package to another requires engineering triaging. If maintainers of the Qt package do this, CVEs will be marked by them as applicable.

    We provide a BSP Maintenance service where our engineering team does the triaging of CVEs. This service could be also used to triage Chromium CVEs for QtWebEngine.

15. **How does the vulnerability report get updated to our project account in Vigiles? Does it update automatically or do we/does the developer need to update the report as necessary?**

    To obtain an updated Vigiles vulnerability report, you have several options including:

    - You can push the software manifest to your Vigiles account every time you run a Yocto build or request a security report using Yocto BitBake commands. When you rerun the build on the same Yocto image, the software manifest can be updated in place. This way, if you add another package to your BSP, it gets reflected in the same product Vigiles report. Because Vigiles stores the older versions of the manifest, you can always go back to view and/or generate reports for older manifests.

    - You can subscribe to notifications on new vulnerabilities reported against a manifest. Once a manifest is in Vigiles, you can choose to receive vulnerability notifications daily, weekly or monthly. Vigiles will automatically run a security scan and email you the information based on your cadence preference.

- You have the ability to upload either a new manifest or an updated version of a manifest at any time using the Vigiles UI.

16. Using Vigiles and this product model, who is responsible for fixing/mitigating a vulnerability?

Vigiles assists with the monitoring and tracking of vulnerabilities and available fixes.

The process of triaging identified CVEs and how they apply to your product, the decision to apply available fixes, the implementation of fixes, and the building and testing of the modified Linux product image is the responsibility of you/your engineering team. Additionally, suggested fixes, patch, and mitigation information is not verified by Timesys.

For those wanting to offload this task, we offer a managed BSP Maintenance service.

17. I already have Black Duck. Do I really need Vigiles too?

Black Duck is a good choice to identify and mitigate open source-related risks when all you have is end device binaries to work with. If you are using Yocto or Buildroot, then Vigiles leverages information about exactly what is being built (configurations, patches applied, etc.) to reduce false positives by 95% and reduce CVEs to analyze by 85% as compared to Black Duck. In short, Black Duck users add Vigiles to save many hours of work. Learn more here: https://www.timesys.com/security/software-composition-analysis-embedded-systems/

18. What about vulnerabilities not in the CVE dictionary?

Vigiles does not cover vulnerabilities that are not reported to or published by the CVE Numbering Authorities (CNAs), or “bug” fixes that were missed being identified as vulnerabilities. Additionally, it does not cover undiscovered vulnerabilities. In short, Vigiles is used for ***publicly known*** vulnerabilities.

To achieve the most comprehensive vulnerability data, Timesys recommends that you run static analysis tools, fuzzing tools, monitor mailing lists, issue trackers, and security bulletins / advisories.

19. How can I report an issue?

You can report an issue or submit feedback by creating a support ticket within Vigiles. Typically, issues are addressed within 72 hours. Once the issue is resolved, all Vigiles users benefit from it, so users are encouraged to report any issues. Additionally, issues can be reported to the NVD and/or MITRE.

Glossary of Terms

CNA: CVE Numbering Authorities are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. (Source)

CPE: Common Platform Enumeration is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name. (Source)

CVE: Common Vulnerabilities and Exposures
A vulnerability is a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety). (Source)

A vulnerability that has been assigned a CVE identifier number is colloquially referred to as a CVE.

NVD: The National Vulnerability Database is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics. (Source)

nxp.com/Vigiles
https://community.nxp.com/community/oss-security-maintenance