BSP SECURITY MAINTENANCE —
Best Practices for Vulnerability Monitoring and Remediation

Webinar Q&A Document
April 23, 2020

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **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.

7. **When scanning our source code, does our source code ever get uploaded or is all scanning performed locally with just the vulnerabilities database being cloud based?**

   No. Vigiles does not upload any source code used in your product, so your source code will never leave your computer/premises. Vigiles only uploads the following:

   - Software Bill of Materials (SBOM) including package name, package version, and any patches applied to the package
   - Linux kernel configuration (option)
   - U-Boot configuration (option)

   This information gets uploaded to your private account on LinuxLink, where Vigiles performs the security scan and generates the reports. The information that you've uploaded and the vulnerability report(s) are not shared with anyone other than your team members.

8. **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.

9. **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.

10. **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.

11. **Using Vigiles, who is responsible for fixing/mitigating a vulnerability? Can Vigiles help me to apply the fix automatically?**

    Vigiles assists with 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.

    If you/your team want to offload this task, we offer a managed BSP Maintenance Service.

12. **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.

13. **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 discussed during the presentation (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.

14. **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.

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

    First, let me start by saying 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.

16. **Are the approximate 350 new CVEs per week you mentioned during the presentation a general number or just the number of CVEs reported against the Linux kernel mainline?**

    The 350 vulnerabilities/week refer 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.

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

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