Best practices for triaging Common Vulnerabilities & Exposures (CVEs) in embedded systems

Webinar Q&A Document
August 27, 2020

1. **Does CVSS apply to vulnerabilities in embedded devices similar to how it is applicable to web applications?**

   Yes. CVSS scores have been in use for a long time in web programming when assessing security risks, and they apply in a similar way to embedded. When NVD analysts review a new CVE, they enter the base metrics of the CVSS.

   Taking the attack vector component of the base metrics as an example, if your device is an IoT device, then the network attack vector is important to consider. If the embedded device is an air gapped device, then physical/local attack vectors are important. Similarly, for headless devices without any local user access, local attack vectors can be ignored. Such filtering can be done using Vigiles.

   In addition, the base metrics also provide the CVE impact in terms of confidentiality, integrity and availability. Depending on your product/organizational requirements, you can set the environmental metrics for the CVE to develop custom CVSS scores, enabling you to better reflect the risk/severity for your product. This is something which tools like Vigiles can help with.

2. **Does the scope metric include privilege escalation?**

   The Base metrics are evaluated and entered by NVD analysts. So depending on the specific vulnerability, if the privilege escalation can lead to affecting other components, then the scope is marked as changed (eg: https://nvd.nist.gov/vuln/detail/CVE-2019-18928) otherwise, it remains unchanged (eg: https://nvd.nist.gov/vuln/detail/CVE-2020-15149).

3. **Does Vigiles support scanning and finding out all software packages (OSS and own) in a product in order to automate the creation of a Software Bill of Materials (SBOM)?**

   Vigiles generates a software manifest/Bill of Materials based on the Yocto or Buildroot rules for creating a final product build which are set in place during development. This ensures the information for software components used in the product is accurate and complete (eg. software versions, patches applied, etc.). Included in the information collected and captured by Vigiles in its generated SBOM is software licensing.

   So then, to answer the question, yes. The Vigiles SBOM captures information on OSS and non-OSS packages used in a product. This information can be used by your team to track your product software composition.

   Vigiles also supports uploading a Software Bill of Materials (SBOM) in .CSV format or generating one using the web wizard.

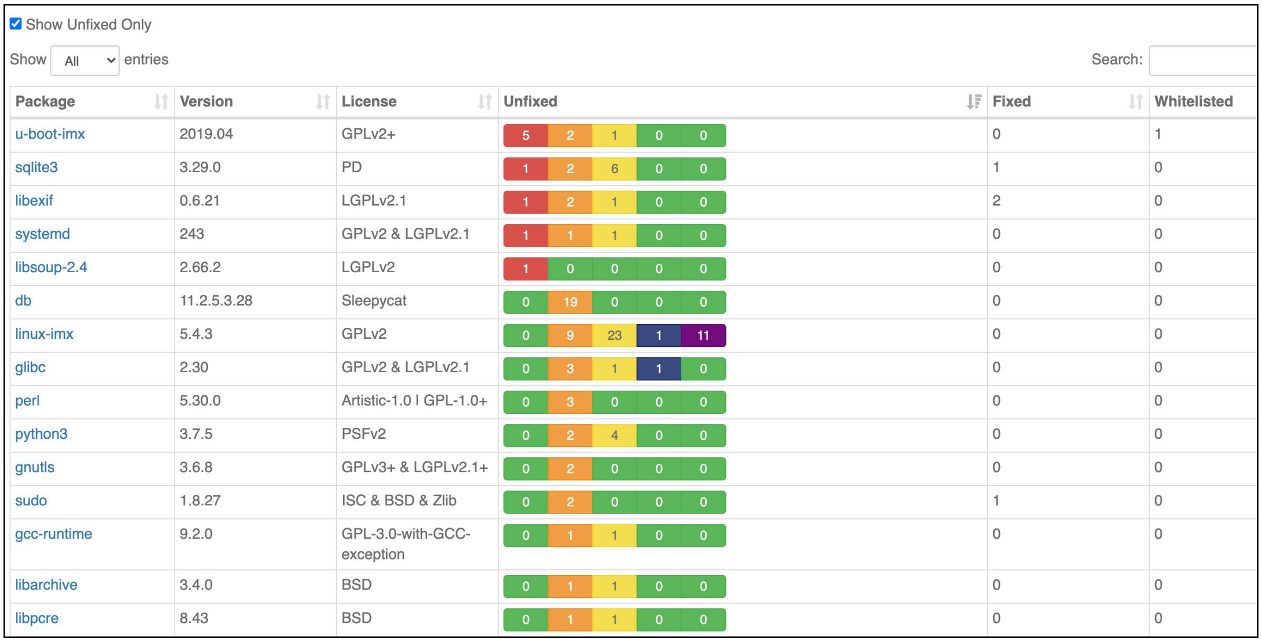
4. **During the session, you mentioned the "Licensing Information." Does this mean that Vigiles can extract the appropriate license type for used OpenSource software packages and/or copyright statements that are required to be reproduced?**

   Vigiles extracts license information from Yocto / Buildroot for packages included in your target image. The license information is pulled from the build system artifacts.

   Vigiles does not scan source code, extract copyright information or look for license violations.

5. **Can you show an example of the license information provided by Vigiles for OSS packages?**

   Below is a screen capture of a sample Vigiles report with licensing information.



☑ Show Unfixed Only

Show All entries

Search:

Package	Version	License	Unfixed	Fixed	Whitelisted
u-boot-imx	2019.04	GPLv2+	5 2 1 0 0	0	1
sqlite3	3.29.0	PD	1 2 6 0 0	1	0
libexif	0.6.21	LGPLv2.1	1 2 1 0 0	2	0
systemd	243	GPLv2 & LGPLv2.1	1 1 1 0 0	0	0
libsoup-2.4	2.66.2	LGPLv2	1 0 0 0 0	0	0
db	11.2.5.3.28	Sleepycat	0 19 0 0 0	0	0
linux-imx	5.4.3	GPLv2	0 9 23 1 11	0	0
glibc	2.30	GPLv2 & LGPLv2.1	0 3 1 1 0	0	0
perl	5.30.0	Artistic-1.0 I GPL-1.0+	0 3 0 0 0	0	0
python3	3.7.5	PSFv2	0 2 4 0 0	0	0
gnutls	3.6.8	GPLv3+ & LGPLv2.1+	0 2 0 0 0	0	0
sudo	1.8.27	ISC & BSD & Zlib	0 2 0 0 0	1	0
gcc-runtime	9.2.0	GPL-3.0-with-GCC-exception	0 1 1 0 0	0	0
libarchive	3.4.0	BSD	0 1 1 0 0	0	0
libpcre	8.43	BSD	0 1 1 0 0	0	0

   You can view a sample of all the information Vigiles provides in a vulnerability report here: https://www.timesys.com/webinars/imx8mnevk-core_2020-08-25T18_47_38.904153.pdf

   You are also encouraged to sign up for a free account and give Vigiles a try with your own BSP. The link to sign up is https://www.timesys.com/register-nxp-vigiles/

6. **How does using NXP Vigiles help lower the triaging effort?**

   Typically, without a tool to assist with vulnerability management, the process of monitoring, triaging and mitigating can take 12 to 15 man months a year. With Vigiles, that effort is greatly reduced. In part because there's a process that is very well supported by the tools, and there is information that the tool makes available to engineers during that process.

   With intuitive filtering capability (based on attack vector, kernel / u-boot config, CVSS score, patch status, custom severity score, hardware platform / OS) and information regarding fixes, the vulnerability management and mitigation effort using Vigiles can probably be reduced to 1 or 2 months a year, which is a significant reduction in the effort.

7. **Can existing triage info be imported into Vigiles?**

   If the user has existing triage data available, it can be imported into Vigiles in the form of .csv file. This way, users can seamlessly transition from their tools/process to using Vigiles.

8. **Are there any suggestions on triaging CVEs that have sparse information in the description/links?**

   Vigiles provides additional vulnerability details that can assist with the triage process. However, one could also leverage work done by some of the major Linux distributions such as Ubuntu, Debian, Red Hat, as they also provide that type of information.

9. **How are CVE fixes suggested by Vigiles?**

   For available CVE fixes, Vigiles provides one of the following:

   - Upgrade information — Vigiles provides the information for the latest version of the package that includes the CVE fix.
   - Patch link — Vigiles provides a direct link to a repository containing the fix.
   - Configuration option — If a CVE applies to a package component (e.g. driver in a Linux kernel), Vigiles will provide information for how the CVE can be mitigated (e.g. CVE can be mitigated by removing the driver from kernel configuration).

10. **How is Vigiles different from the Yocto Project cve-check tool?**

    Indeed, the Yocto Project has a cvecheck tool built in which allows for rudimentary security checks on the BSP. Unfortunately, the Yocto cve-checker lacks accuracy and coverage, and therefore, is not recommended for comprehensive, accurate security assessment.

    Vigiles uses multiple sources of security feeds (apart from NVD) and has a security team that curates the information to reduce false positives and improve coverage. When we compared Vigiles with Yocto cve-check, we found 40%+ security information either missing or reported wrong by cve-check.

    Further, Vigiles is a complete end-to-end vulnerability management tool that provides:

    - Email alerts for new vulnerabilities based on your preferred frequency.
    - Intuitive prioritization and filtering mechanisms (kernel/U-Boot config filter, attack vector filter, CVSS filter, etc.).
    - Complete vulnerability management workflow: history; exported reports in .pdf, .xls, and .csv formats; custom notes; whitelist, and comparision between builds/reports.
    - Team collaboration/sharing
    - Links to applicable patches and recommends minimum version upgrades with relevant fixes

    All of the above are not possible using the Yocto cve-checker. You can see a full list of Vigiles features at https://www.nxp.com/docs/en/supporting-information/COMPARE-VIGILES-SECUTIRY_MONITORING.pdf

11. **Does Vigiles only support Linux? Can it be used for RTOS or baremetal programs/libraries?**

    Behind Vigiles is a curated database of CVEs, which is maintained by Timesys and based on CVEs reported in public databases. The Timesys database is not limited to embedded Linux, so it also holds CVEs for non-Linux vulnerabilities. As such, Vigiles can be used to assess security vulnerabilities for RTOS and other operating systems, given that vulnerabilities for these systems are reported in public CVE databases.

    Vigiles supports uploading a Software Bill of Materials (SBOM) or generating one using the web wizard where your RTOS components and other libraries can be selected/uploaded for monitoring vulnerabilities.

12. **How frequently is the Vigiles database updated with vulnerabilities information?**

    The Vigiles database is updated daily.

    In alignment with the Vigiles database updates, daily is the most frequent cadence for security alert email notifications offered as part of Vigiles subscription.

13. **Is Vigiles an NXP product or a Timesys product?**

    The technology behind Vigiles product has been developed and is maintained by Timesys.

14. **Is there a recording of the previous webinar mentioned in this session?**

    Yes. You can find the recordings for the two previous NXP webinars at:

    BSP Security Maintenance - Best Practices for Vulnerability Monitoring and Remediation https://www.nxp.com/design/training/bsp-security-maintenance-best-practices-for-vulnerability-monitoring-and-remediation:TIP-BSP-SECURITY-BEST-PRACTICES

    Full Life-Cycle Security Maintenance of Embedded Linux BSPs https://www.nxp.com/design/training/full-life-cycle-security-maintenance-of-embedded-linux-bsps:TIP-FULL-LIFE-CYCLE-SECURITY-MAINTENANCE-D0602

https://www.nxp.com/support/support/nxp-engineering-services/vigiles-software-keeping-your-linux-bsp-secure:VIGILES

https://www.nxp.com/support/support/nxp-engineering-services/bsp-lifecycle-maintenance:BSP-LIFECYCLE-MAINTENCE

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