Eclipse oniro
CVE-checking an entire distribution

Marta Rybczynska
Yocto Project Summit 2022.5
WHAT IF…

- You want to check your distribution for known security issues (CVEs)
- You want to do security reporting
  - Which layer, how the number of issues changes over time
- You want to monitor issues over time
  - New ones, a number of issues above a severity level…
Oniro is an Eclipse project

A distro for IoT/embedded products
- Based on OpenEmbedded/Yocto, of course

Multi-scenarios
- Multi-OS: Linux, Zephyr...
- Multi-board

You can learn more from a presentation earlier today “Oniro Project – A Yocto-based product-ready distribution”
A REFRESHER: WHAT IS CVE?

- **Common Vulnerability Enumeration (CVE)** - a standard for naming security issues
  - Known issues only
  - Someone needs to request a number – there are vulnerabilities without a CVE number

- **Naming format**: `CVE-YYYY-NNNN` eg. `CVE-2022-12345`

- **Refers to a specific issue, in a specific package and configuration**
  - Example: a CVE in vim

- **Website**: https://www.cve.org
A REFRESHER: WHAT IS NVD?

- **National Vulnerability Database (NVD)** – a database with more information about CVEs
  - *Includes product names (CPE standard)*
  - *Includes references to fixes, advisories etc*

- **Yocto’s CVE-checker** uses the NVD

- **Website**: [https://nvd.nist.gov](https://nvd.nist.gov)

CVE-2022-27404 Detail

UNDERGOING REANALYSIS

This vulnerability has been modified and is currently undergoing reanalysis. Please check back soon to view the updated vulnerability summary.

Current Description

FreeType commit 1e2eb65048f75c64b68708eved6cede904c31f3b2f was discovered to contain a heap buffer overflow via the function sfmt_init_face.

Severity

CVSS Version 3.1

- NIST: NVD
- Base Score: 9.8 CRITICAL

CVSS 3.x Severity and Metrics:

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools
NVD status for 2022–27404 as of May 13, 2022:

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

<table>
<thead>
<tr>
<th>Hyperlink</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://gitlab.freedesktop.org/freetype/freetype/-/issues/1138">https://gitlab.freedesktop.org/freetype/freetype/-/issues/1138</a></td>
<td>Exploit</td>
</tr>
<tr>
<td><a href="https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EFPNRKDLCXHZVYYQLQMP44UHLU32GA6Z/">https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EFPNRKDLCXHZVYYQLQMP44UHLU32GA6Z/</a></td>
<td>Vendor Advisory</td>
</tr>
<tr>
<td><a href="https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FDU2FOEMCEF6WR6ZB1H5MT507FAK6UP/">https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FDU2FOEMCEF6WR6ZB1H5MT507FAK6UP/</a></td>
<td>Third Party Advisory</td>
</tr>
</tbody>
</table>
NVD status for 2022–27404 as of May 13, 2022:

<table>
<thead>
<tr>
<th>Known Affected Software Configurations</th>
<th>CPE 2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration 1</strong></td>
<td></td>
</tr>
<tr>
<td>- cpe:2.3:a:freetype:freetype:<em>:</em>:<em>:</em>:<em>:</em></td>
<td>Up to (excluding) 2.12.0</td>
</tr>
<tr>
<td>- Show Matching CPE(†)</td>
<td></td>
</tr>
</tbody>
</table>

| **Configuration 2**                    |         |
| - cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:* |         |
| - Show Matching CPE(†)                 |         |
| - cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:* |         |
| - Show Matching CPE(†)                 |         |
WHY DO A CVE-CHECK?

- Find out which dependencies you need to upgrade
  - Or which to remove...
- Update your information: vulnerabilities go public every day
- Mix with other approaches, like:
  - Hardening
  - Static analysis
CVE-CHECK IN YOCTO

- Add to your conf/local.conf:
  - `INHERIT += "cve-check"`

- Build your image as usual
  - The tool will download the database (cve-update-db-native)
  - Then do a check that lasts 1–3 minutes

- Results:
  - Log files (cve.log) for each recipe
  - A common log file for each image (yourimage.cve)
CVE-CHECK TEXT FORMAT: AN EXAMPLE

Layer: meta
Package Name: linux-yocto
Package Version: 5.13.12+gitAUTOINC+c38435a3ca_49ec738aa7
CVE: CVE-2021-3564
CVE Status: Unpatched
CVE Summary: A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVSS v2 Base Score: 2.1
CVSS v3 Base Score: 5.5
Vector: LOCAL
More Information: https://nvd.nist.gov/vuln/detail/CVE-2021-3564
Why?
- Allow easy post-processing, statistics

Why JSON?
- Related tools use JSON in Yocto already
  - Notably the SPDX tool
- The new CVE format is JSON (5.0, expected deployment this year – in 2022)
NEW VARIABLES IN CVE-CHECK

○ Legacy text format:
  - `CVE_CHECK_FORMAT_TEXT` enabled by default

○ New JSON format:
  - `CVE_CHECK_FORMAT_JSON` enabled by default in master, disabled in dunfell

○ Coverage statistics, only with the JSON format
  - `CVE_CHECK_COVERAGE` enabled by default
Reminder: the package name might differ from the name in the NVD database (the CPE used)

What is the old format missing?
- Nothing about packages without CVEs (possible name mismatches!)
- Nothing about which product name was used
CVE-CHECK JSON FORMAT: AN EXAMPLE

```json
{
  "name": "ncurses-native",
  "layer": "meta",
  "version": "6.3",
  "products": [
    {
      "product": "ncurses",
      "cvesInRecord": "Yes"
    }
  ],
  "issue": [
    {
      "id": "CVE-2017-10684",
      "summary": "In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack."
    }
  ],
  "CVE-CHECK JSON FORMAT: AN EXAMPLE

Building together a fully-connected all-scenario intelligent ecosystem

```
● Cve-check works fine for a single image
  - At Oniro we have a number of images, so not practical
  - And only tests packages included into the image
● We’ve found out that some layers weren’t prepared for the “world” build
  - Fixes upstream
NEXT STEPS

- More tooling
  - On top on the JSON format
- Pending issues
  - On meta-zephyr still need `--runall=do_cve_check`
- Missing features
  - Scan recipes with multiple libraries/tools (eg. meta-zephyr)
  - Take library copies into account
• Davide Gardenal – work on “world” for cve-check
• Andrei Gherzan – help with various low-level subjects
• Steve Sakoman – discussions on the CVE reporting scripts
□ CVE check in JSON
  − In the Yocto kirkstone branch near you
□ Oniro websites:
□ Source code:
  − https://gitlab.eclipse.org/eclipse/oniro-core/oniro
Eclipse oniro
CVE-checking an entire distribution

Marta Rybczynska
Yocto Project Summit 2022.5
• 20 years in software development and Open Source
  – Including 15 years in embedded
• PhD in Telecommunications - on network security
• Worked in embedded product development, silicon...
  – Now moved to distributions
• Guest author at LWN
• Contributing to Oniro from April 2021, consulting for OSTC