Securing a Yocto-based Distribution

Marta Rybczynska
Security lead for AllScenariosOS OSTC/Huawei

#lfelc @mrybczynska
Marta Rybczynska: about me

• Security researcher background, PhD
  – Specialization in network security
• 20 years experience in OpenSource
  – Including: former Vice-President of KDE e.V
• Worked on hardware-related issues (kernel porting, low-level networking, intrusion detection etc)
• Currently involved in OpenSSF (esp. Best practices group)
Millions of IoT Devices Exposed to Attacks Due to Cloud Platform Vulnerability

Source: https://www.securityweek.com/millions-iot-devices-exposed-attacks-due-cloud-platform-vulnerability

Critical Flaws in Millions of IoT Devices May Never Get Fixed

Amnesia:33 is the latest in a long line of vulnerabilities that affect countless embedded devices.

Source: https://www.wired.com/story/amnesia33-iot-vulnerabilitiesmay-never-get-fixed/
You're Doing IoT RNG

Dan Petro Allan Cecil on Aug 5, 2021 11:43:40 AM

There's a crack in the foundation of Internet of Things (IoT) security, one that affects 35 billion devices worldwide. Basically, every IoT device with a hardware random number generator (RNG) contains a serious vulnerability whereby it fails to properly generate random numbers, which undermines security for any upstream use.

Source: https://labs.bishopfox.com/tech-blog/youre-doing-iot-rng with a presentation at DEFCON
Scary? Examples of issues from...

- External suppliers (the cloud...)
- The code you reuse (network stacks, libraries...)
- Software-hardware interface
- Your own code
What can you do?
What will we talk about?

• Yocto security basics
• AllScenariosOS specifics
• Into the details...
  – CVE check
  – Meta-security & hardening
• Community work in progress
• Next steps
Yocto security basics – a subjective view (1/2)

• Easy to add new software
  – With all dependencies
  – Risk of including buggy (vulnerable) components

• A choice of security tools available
  – Layers like: meta-security, meta-selinux, meta-virtualization
  – Some tools require knowledge to configure/understand output
• LTS exists
  – New process, starting from dunfell (released in April 2020)
  – A set of layers, other layers might have their own LTS policy
  – Support for at least 2 years, possibly non-overlapping with the next LTS
  – ...but doesn’t include the packages/layers you added :)

• Documentation
  – **What should be your priorities?** Answer (somewhat) complicated to find
  – More work planned, see for example Bugzilla issue https://bugzilla.yoctoproject.org/show_bug.cgi?id=14509
What can you have out of the box? (and easily)

- **Compiler flags**
  - Just add require
    ```
    conf/distro/include/security_flags.inc into your local.conf or distribution configuration
    ```

- **Remove debug flags**
  - In IMAGE_FEATURES, make sure you do **NOT** have “debug-tweaks”

- **Users/passwords**
  - Disable root login, add regular user(s)
  - Set up passwords, ideally different for each device OR require change at first login
What is AllScenariosOS?
AllScenariosOS in a nutshell

• A source-based distribution
  – Multi-kernel, including Linux, Zephyr and more
  – Using Yocto, of course :)

• Targetting IoT
  – Communication between different classes of devices
  – Privacy and security as part of main goals

• To learn more see Davide Ricci presentation Meet All Scenarios OS: A Distributed O.S. with Feet on the Ground on September 28, 2021 at 9am PDT
  https://sched.co/lAMZ
AllScenariosOS security: work done or in progress

• Hardening by default
  – Linux kernel options (*), sysctl defaults
  – Compiler options

• Image hardening
  – Removing unneeded services
  – Permission adjustments

• Tooling
  – Removing unneeded services
  – CVE checking (*)

(*) will talk about this in more details
Into the details: CVE check
CVE... what?

- CVE = Common Vulnerabilities and Exposures
  - A database of vulnerabilities, each with unique name
  - Operated by Mitre
  - Identifier format: CVE-YEAR-Digits
  - Search: [https://cve.mitre.org/cve/search_cve_list.html](https://cve.mitre.org/cve/search_cve_list.html)

- Contains
  - The ID, a description, product name, vulnerable versions
  - Score(s): how serious it is
  - References (links to resources, like a mailing list post)
  - Search: [https://cve.mitre.org/cve/search_cve_list.html](https://cve.mitre.org/cve/search_cve_list.html)
### Search Results

There are 166 CVE Records that match your search.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2021-38604</td>
<td>In libt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.</td>
</tr>
<tr>
<td>CVE-2021-35942</td>
<td>The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atol was used but strtol should have been used to ensure correct calculations.</td>
</tr>
<tr>
<td>CVE-2021-3470</td>
<td>A heap overflow issue was found in Redis in versions before 5.0.10, before 6.0.9 and before 6.2.0 when using a heap allocator other than jemalloc or glibc's malloc, leading to potential out of bound write or process crash. Effectively this flaw does not affect the vast majority of users, who use jemalloc or glibc malloc.</td>
</tr>
<tr>
<td>CVE-2021-33574</td>
<td>The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been</td>
</tr>
</tbody>
</table>
**CVE-ID**

**CVE-2021-38604** [Learn more at National Vulnerability Database (NVD)](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38604)
- CVSS Severity Rating
- Fix Information
- Vulnerable Software Versions
- SCAP Mappings
- CPE Information

**Description**

In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.

**References**

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC: https://sourceware.org/bugzilla/show_bug.cgi?id=28213
- MISC: https://sourceware.org/git/?p=glibc.git;a=commit;h=4cc79c217744743077bf7a0ec5e0a4318f1e6641
- MISC: https://sourceware.org/git/?p=glibc.git;a=commit;h=b805aebd42364fe696e417808a700fdb9800c9e8

**Assigning CNA**

MITRE Corporation

**Date Record Created**

20210812

Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
What a developer should know about CVEs

• Given only if someone requests
  – You can have a security issue without a CVE number

• Database content changes
  – ID numbers are reserved, content released when issue is public
  – Sometimes mismatches, errors (eg. vulnerable versions, product names...)

• Other databases exist
  – NVD: CVE list with additional information
    https://nvd.nist.gov/vuln/search
CVE-2021-38604 Detail

Current Description
In libt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.

Severity
CVSS Version 3.1
- NIST: NVD
- Base Score: 7.5 (HIGH)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS Version 2.0
- 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
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://sourceware.org/gbzilla/show_bug.cgi?id=28213">https://sourceware.org/gbzilla/show_bug.cgi?id=28213</a></td>
<td>Issue Tracking</td>
</tr>
<tr>
<td></td>
<td>Patch Third Party Advisory</td>
</tr>
<tr>
<td><a href="https://sourceware.org/git/?p=glibc.git;a=commit">https://sourceware.org/git/?p=glibc.git;a=commit</a>; h=ac4c2177447f3e77b7f97a0fe3e19a6f6e6641</td>
<td>Mailing List Patch Third Party Advisory</td>
</tr>
<tr>
<td><a href="https://sourceware.org/git/?p=glibc.git;a=commit">https://sourceware.org/git/?p=glibc.git;a=commit</a>; h=ba85eabdb2364ede6564e17808a70065b9800c3e8</td>
<td>Mailing List Patch Third Party Advisory</td>
</tr>
</tbody>
</table>

#lfecl
CVE-2021-38604 Detail

Current Description
In libt in the GNU C Library (aka glibc) through 2.34, sysefs/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY(_:REM to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.

Severity
CVSS Version 3.0
CVSS Version 2.0

CVSS 3.0 Severity and Metrics:

NIST: NVD
Base Score: 7.5 HIGH
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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://sourceware.org/bugzilla/show_bug.cgi?id=28213">https://sourceware.org/bugzilla/show_bug.cgi?id=28213</a></td>
<td>Issue Tracking, Patch, Third Party Advisory</td>
</tr>
<tr>
<td><a href="https://sourceware.org/git/?p=glibc.git;a=commit;h=4cc79c21774474307f7bfa0e0c3e60a311f8c876441">https://sourceware.org/git/?p=glibc.git;a=commit;h=4cc79c21774474307f7bfa0e0c3e60a311f8c876441</a></td>
<td>Mailing List, Patch, Third Party Advisory</td>
</tr>
<tr>
<td><a href="https://sourceware.org/git/?p=glibc.git;a=commit;h=bb065adb42364fe896e417808a700fd5b9800c3e8">https://sourceware.org/git/?p=glibc.git;a=commit;h=bb065adb42364fe896e417808a700fd5b9800c3e8</a></td>
<td>Mailing List, Patch, Third Party Advisory</td>
</tr>
</tbody>
</table>
CVE-2021-38604 Detail

Current Description

In libnl in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.

Severity

CVSS Version 3.1

NVD: NVD

Base Score: 7.5


CVSS 3.0 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

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 in any case 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.

Hyperlink


https://sourceware.org/bugzilla/show_bug.cgi?id=28213

https://sourceware.org/git/?p=glibc.git;a=commit;h=4cc79c2177447430777bf7a0e5e0a4318f1e6641

https://sourceware.org/git/?p=glibc.git;a=commit;h=b805aebd42364fe696e417808a700fdbc9800c9e8

Weakness Enumeration

CWE-ID | CWE Name | Source
--- | --- | ---
CWE-476 | NULL Pointer Dereference | NIST

Known Affected Software Configurations

Configuration 1

cpe:2.3:a:gnu:glibc:*

Up to (including) 2.34
Cve-check in Yocto: HOWTO

• 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) files for each recipe
  – A common log file for each image (yourimage.cve)
Cve-check console output (fragment)

WARNING: sqlite3-3_3.36.0-r0 do_cve_check: Found unpatched CVE (CVE-2021-36690), for more information check /yocto-mainline/poky/build/tmp/work/core2-64-poky-linux/sqlite3/3_3.36.0-r0/temp/cve.log


WARNING: flex-native-2.6.4-r0 do_cve_check: Found unpatched CVE (CVE-2019-6293), for more information check /yocto-mainline/poky/build/tmp/work/x86_64-linux/flex-native/2.6.4-r0/temp/cve.log

WARNING: libarchive-native-3.5.1-r0 do_cve_check: Found unpatched CVE (CVE-2021-36976), for more information check /yocto-mainline/poky/build/tmp/work/x86_64-linux/libarchive-native/3.5.1-r0/temp/cve.log

WARNING: qemu-system-native-6.0.0-r0 do_cve_check: Found unpatched CVE (CVE-2019-12067 CVE-2020-35503 CVE-2021-20255 CVE-2021-3507 CVE-2021-3713), for more information check /yocto-mainline/poky/build/tmp/work/x86_64-linux/qemu-system-native/6.0.0-r0/temp/cve.log

Image CVE report stored in: /yocto-mainline/poky/build/tmp/deploy/images/qemux86-64/core-image-minimal-qemux86-64-20210903144352.rootfs.cve
Cve-check output file (fragment)

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
Cve-check output file (fragment)

LAYER: meta
PACKAGE NAME: linux-yocto
PACKAGE VERSION: 5.13.12+gitAUTOINC+c38435a3ca_49ec738aa7
CVE: CVE-2019-14901
CVE STATUS: Patched
CVE SUMMARY: A heap overflow flaw was found in the Linux kernel, all versions 3.x.x and 4.x.x before 4.18.0, in Marvell WiFi chip driver. The vulnerability allows a remote attacker to cause a system crash, resulting in a denial of service, or execute arbitrary code. The highest threat with this vulnerability is with the availability of the system. If code execution occurs, the code will run with the permissions of root. This will affect both confidentiality and integrity of files on the system.
CVSS v2 BASE SCORE: 10.0
CVSS v3 BASE SCORE: 9.8
VECTOR: NETWORK
Research on cve-check

• How many packages have reported CVEs? (Patched or Unpatched)
  – Around half of them

• And others?
  – Either no known CVEs (and some horror stories)
  – Or a product name mismatch (fixes in progress)

• Wrote an extension to help: first version at https://lists.openembedded.org/g/openembedded-core/message/154677
LAYER: meta
PACKAGE NAME: libsdl2-native
PACKAGE VERSION: 2.0.14
CVES FOUND IN RECIPE: Yes
  PRODUCT: simple_directmedia_layer (Yes)
  PRODUCT: sdl (No)
Into the details: meta-security and hardening
Security-related layers in Yocto

- **meta-security**
  - A collection of layers and tools

- **meta-selinux**
  - Support for SELinux

- **meta-virtualization**
  - Virtualized images support, including KVM, Xen...
Meta-security sublayers (as of master, Aug 2021)

- meta-hardening
- meta-integrity
- meta-parssec
- meta-security-compliance
- meta-security-isafw
- meta-tpm
Adding meta-security or sublayers

- Add meta-security and its sublayers, like meta-security-compliance
- Into your configuration (warning: new append syntax!)
  - DISTRO_FEATURES:append = "security"
- Enable new packages, for example
  - IMAGE_INSTALL:append = "lynis checksec"
Special case: meta-hardening

- Example of a hardened distro
- Contains
  - No root login
  - Changed password
  - Some permission changes (eg. umask)
  - Login timeout, minimum password length etc
Using meta-hardening

• Add the layer
• Adjust your configuration
  – DISTRO = "harden"
• Build the distro, eg.
  – bitbake harden-core-minimal
Hardening and meta-security in AllScenariosOS

• No meta-hardening in dunfell
  – And we want to have those options by default
  – Backported directly to the main distro layer
  – More permission changes added (and even more planned!)

• Meta-security added to the default layers
  – The default set of tools under definition still
  – System analysis done with tools (included!) like lynis and checksec
Linux kernel hardening in AllScenariosOS

- Based on Kernel Self Protection Project: http://kernsec.org/wiki/index.php/Kernel_Self_Protection_Project/Recommended_Settings with some additions and changes
If you want to know more...

- « Security Hardening with OpenEmbedded/ YoctoProject » by Scott Muray
  - Contains lists of packages available from meta-security layers

- Yocto project security wiki
Community work in progress (in Yocto)
Community work of interest in Yocto/OpenEmbedded

- SBOM generation
  - Submitted
    https://lists.openembedded.org/g/openembedded-core/message/155561

- More security documentation
  - Bugzilla “Add security configuration documentation”
    https://bugzilla.yoctoproject.org/show_bug.cgi?id=14509
Next steps
Next steps

• Secure boot and image verification
  – With meta-integrity
  – Likely reusing work from the LEDGE group of Linaro
    https://github.com/Linaro/meta-ledge

• Checking for packages to update (automated!)

• Integration of findings from security checks with IP compliance
  – Including easier to parse output of cve-check

• Upstreaming of various fixes and changes (some landed already)
Lessons learnt

• Removing packages might be harder than adding them
  – Which packages really aren’t needed? What has been pulled in as a dependency
  – Requires careful dependency graph analysis
• Interested to see meta-hardening change into an option in DISTRO_FEATURES
• Large changes in security related layers between Yocto versions
  – Dunfell had no meta-hardening
  – Cve-check patch application non-trivial between dunfell and master
If you want to learn more about security

• Many packages ready to use in Yocto/OE
  – You might find exactly what you need (and the docs!)
• Hundreds of pages available online
• Open Source Security Foundation (OpenSSF) resources
  https://openssf.org/
  – Various working groups on different subjects
Time for Questions!