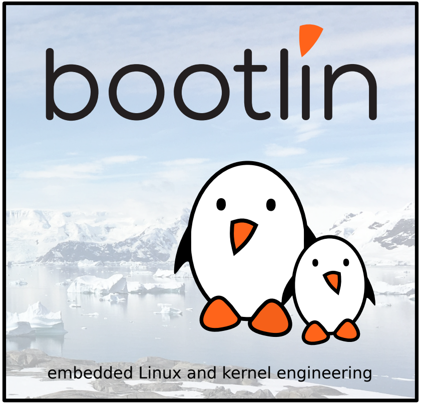
Live Embedded Event, June 3rd 2021

Security vulnerability tracking tools in Buildroot

Thomas Petazzoni
thomas.petazzoni@bootlin.com



Who is speaking ?

- Thomas Petazzoni
- Co-owner and CEO at Bootlin
- Joined in 2008, employee #1
- Embedded Linux engineer and trainer
- Open-source contributor
- **Buildroot co-maintainer**, contributor since 2008, contributed 4000+ patches
- Based in Toulouse, France

Agenda

- What is Buildroot?
- Build systems and security vulnerabilities: which relationship?
- The acronym soup: NVD, CVE and CPE
- Security vulnerability tracking in Buildroot
- Limitations and future work
- Q&A

What is Buildroot ?

- Embedded Linux build system
  - Automates the process of cross-compiling a complete customized Linux system for embedded platforms
  - Root filesystem with applications/libraries, cross-compilation toolchain, bootloader and kernel images
  - Same role as OpenEmbedded/Yocto, OpenWrt, PTXdist, etc.
- 2800+ packages, for the most popular open-source libraries/applications
- Simple to use and understand
- Written in *make* + *kconfig*
- 4 releases per year, one release maintained during one year with security updates
- Active community, large user base in the insdustry

Buildroot quickstart

```
$ git clone git://git.buildroot.org/buildroot
$ cd buildroot
$ git checkout 2021.02.2
```

Buildroot quickstart

```
$ git clone git://git.buildroot.org/buildroot
$ cd buildroot
$ git checkout 2021.02.2

$ make qemu_aarch64_virt_defconfig
```

Buildroot quickstart

```
$ git clone git://git.buildroot.org/buildroot
$ cd buildroot
$ git checkout 2021.02.2

$ make qemu_aarch64_virt_defconfig

$ make menuconfig
... customize your selection of packages ...
```

Buildroot quickstart

```
$ git clone git://git.buildroot.org/buildroot
$ cd buildroot
$ git checkout 2021.02.2

$ make qemu_aarch64_virt_defconfig

$ make menuconfig
... customize your selection of packages ...

$ make
```

Buildroot quickstart

```
$ git clone git://git.buildroot.org/buildroot
$ cd buildroot
$ git checkout 2021.02.2

$ make qemu_aarch64_virt_defconfig

$ make menuconfig
... customize your selection of packages ...

$ make
```

Ready to use images in `output/images`

Build systems and security vulnerabilities

- Build systems are responsible for **automatically** downloading, building and integrating all the system components
- Typically includes a **large number** of open-source libraries/applications + some in-house/proprietary components
- Number of open-source components can get quite large on a typical embedded systems → **difficult to manually track** all security vulnerabilities
- Just like build systems usually offer *license compliance* tooling, it makes sense to also have **security vulnerability tracking** tooling.

NVD, NIST, CVE, CPE: the acronym soup

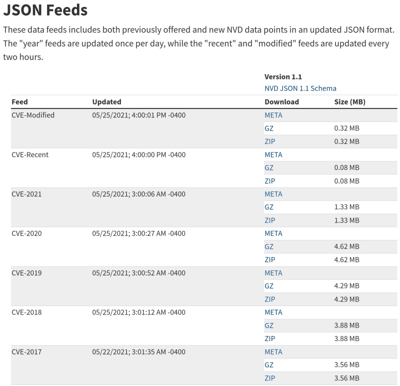
- **NVD** = National Vulnerability Database
- Maintained by **NIST**, National Institute of Standards and Technology, US
- https://nvd.nist.gov/
- *The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). 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.*

NIST
NVD MENU
NATIONAL VULNERABILITY DATABASE
NVD
CVMAP
CVSS
NVD Release of CVMAP
CVSS Version 3.1 Official Support!
New NVD CVE/CPE API and Legacy SOAP Service Retirement!

The NVD 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.

NVD, NIST, CVE, CPE: the acronym soup

- **CVE** = Common Vulnerabilities and Exposures
- A reference for publicly-known security vulnerabilities
- Some well-known CVEs
  - CVE-2014-0160, Heartbleed
  - CVE-2017-5754, Meltdown
  - CVE-2020-24588, one of the FragAttacks
- Are generally recognized in the industry as the reference identifiers for known security issues.
- NVD provides a per-year JSON dump of the CVEs at `https://nvd.nist.gov/vuln/data-feeds`



JSON Feeds

These data feeds includes both previously offered and new NVD data points in an updated JSON format. The "year" feeds are updated once per day, while the "recent" and "modified" feeds are updated every two hours.

		Version 1.1 NVD JSON 1.1 Schema	
Feed	**Updated**	**Download**	**Size (MB)**
CVE-Modified	05/25/2021; 4:00:01 PM -0400	META	
		GZ	0.32 MB
		ZIP	0.32 MB
CVE-Recent	05/25/2021; 4:00:00 PM -0400	META	
		GZ	0.08 MB
		ZIP	0.08 MB
CVE-2021	05/25/2021; 3:00:06 AM -0400	META	
		GZ	1.33 MB
		ZIP	1.33 MB
CVE-2020	05/25/2021; 3:00:27 AM -0400	META	
		GZ	4.62 MB
		ZIP	4.62 MB
CVE-2019	05/25/2021; 3:00:52 AM -0400	META	
		GZ	4.29 MB
		ZIP	4.29 MB
CVE-2018	05/25/2021; 3:01:12 AM -0400	META	
		GZ	3.88 MB
		ZIP	3.88 MB
CVE-2017	05/22/2021; 3:01:35 AM -0400	META	
		GZ	3.56 MB
		ZIP	3.56 MB

CVE database entry example: CVE-2020-29074

```
"cve" : {
  ...
  "CVE_data_meta" : {
    "ID" : "CVE-2020-29074",
    "ASSIGNER" : "cve@mitre.org"
  },
 ....
 "configurations" : {
  "CVE_data_version" : "4.0",
  "nodes" : [ {
    "operator" : "OR",
    "children" : [ ],
    "cpe_match" : [ {
      "vulnerable" : true,
      "cpe23Uri" : "cpe:2.3:a:x11vnc_project:x11vnc:0.9.16:*:*:*:*:*:*:*",
      "cpe_name" : [ ]
    } ]
```

→ single version affected, 0.9.16

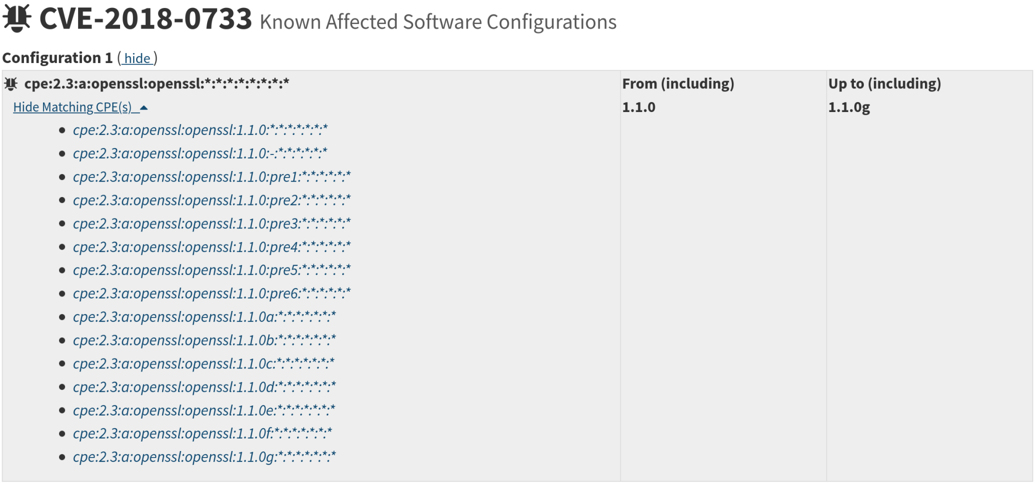
CVE database entry example: CVE-2018-0733

```
"cve" : {
  ...
  "CVE_data_meta" : {
    "ID" : "CVE-2018-0733",
    "ASSIGNER" : "openssl-security@openssl.org"
  },

"configurations" : {
  "nodes" : [ {
    "operator" : "OR",
    "cpe_match" : [ {
      "vulnerable" : true,
      "cpe23Uri" : "cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:*:*",
      "versionStartIncluding" : "1.1.0",
      "versionEndIncluding" : "1.1.0g",
      "cpe_name" : [ ]
    } ]
  } ]
```

→ range of versions affected

CVE-2018-0733 list of affected versions



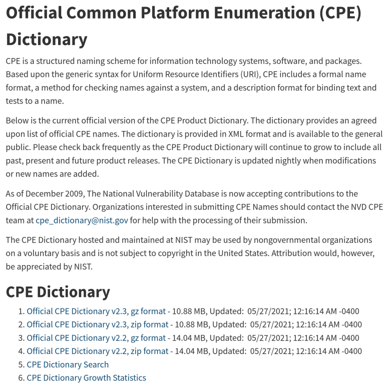
CVE-2018-0733 Known Affected Software Configurations

Configuration 1 (hide)

cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:*:*	**From (including)**	**Up to (including)**
Hide Matching CPE(s) ▲ • *cpe:2.3:a:openssl:openssl:1.1.0:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:-:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:pre1:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:pre2:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:pre3:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:pre4:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:pre5:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0:pre6:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0a:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0b:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0c:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0d:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0e:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0f:*:*:*:*:*:*:** • *cpe:2.3:a:openssl:openssl:1.1.0g:*:*:*:*:*:*:**	**1.1.0**	**1.1.0g**

NVD, NIST, CVE, CPE: the acronym soup

- **CPE** = Common Platform Enumeration
- *structured naming scheme for information technology systems, software, and packages*
- Or put it different: unique identifier for software releases
- `cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>`
- Examples
  - `cpe:2.3:a:ntp:ntp:4.2.8:p3:*:*:*:*:*:*`
  - `cpe:2.3:a:x11vnc_project:x11vnc:0.9.16:*:*:*:*:*:*:*`
- *CPE dictionary* provided by NVD: lists all known software releases, as a huge XML blurb
- Used in the NVD database of CVEs



Official Common Platform Enumeration (CPE) Dictionary

CPE 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.

Below is the current official version of the CPE Product Dictionary. The dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. The CPE Dictionary is updated nightly when modifications or new names are added.

As of December 2009, The National Vulnerability Database is now accepting contributions to the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their submission.

The CPE Dictionary hosted and maintained at NIST may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

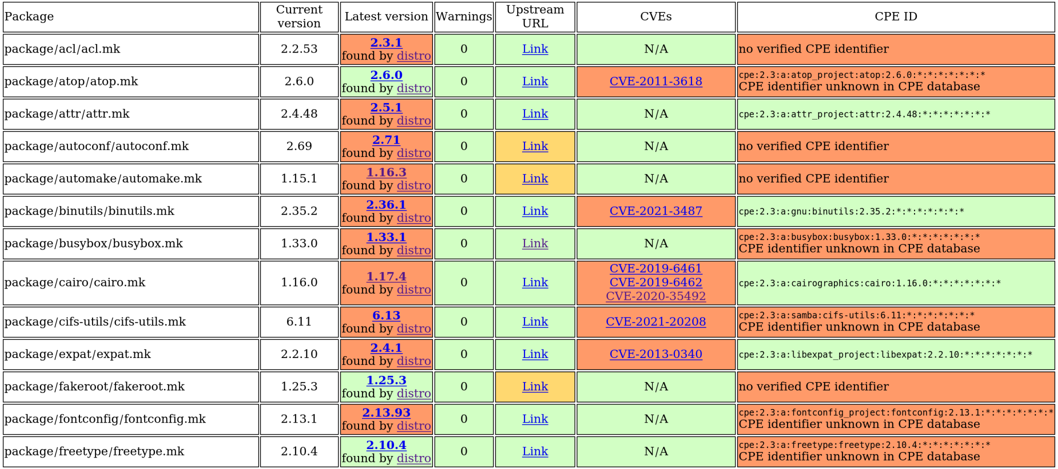
CPE Dictionary

1. Official CPE Dictionary v2.3, gz format - 10.88 MB, Updated: 05/27/2021; 12:16:14 AM -0400
2. Official CPE Dictionary v2.3, zip format - 10.88 MB, Updated: 05/27/2021; 12:16:14 AM -0400
3. Official CPE Dictionary v2.2, gz format - 14.04 MB, Updated: 05/27/2021; 12:16:14 AM -0400
4. Official CPE Dictionary v2.2, zip format - 14.04 MB, Updated: 05/27/2021; 12:16:14 AM -0400
5. CPE Dictionary Search
6. CPE Dictionary Growth Statistics

In Buildroot

- Existing `pkg-stats` tool
  - Originally maintainer-oriented
  - Collects details on the entire package set
  - Existence of license file ? Hash file ? Current packaged version vs. latest upstream version ?
- Extended with:
  - Collecting details only for the packages of the current configuration → useful for users
  - Matching of packages with the NVD databases: CVE and CPE
- `make pkg-stats`
  - Produces JSON and HTML output
  - Downloads NVD database in `$(DL_DIR)/buildroot-nvd/`
- Available since Buildroot 2021.02

pkg-stats output

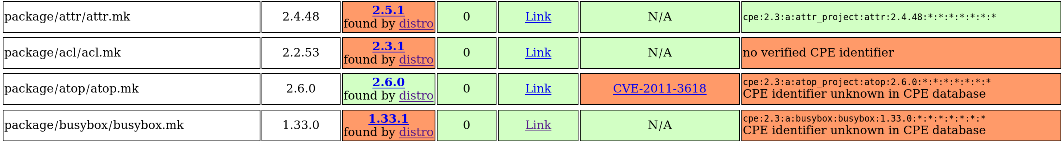


Package	Current version	Latest version	Warnings	Upstream URL	CVEs	CPE ID
package/acl/acl.mk	2.2.53	2.3.1 found by distro	0	Link	N/A	no verified CPE identifier
package/atop/atop.mk	2.6.0	2.6.0 found by distro	0	Link	CVE-2011-3618	cpe:2.3:a:atop_project:atop:2.6.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/attr/attr.mk	2.4.48	2.5.1 found by distro	0	Link	N/A	cpe:2.3:a:attr_project:attr:2.4.48:*:*:*:*:*:*:*
package/autoconf/autoconf.mk	2.69	2.71 found by distro	0	Link	N/A	no verified CPE identifier
package/automake/automake.mk	1.15.1	1.16.3 found by distro	0	Link	N/A	no verified CPE identifier
package/binutils/binutils.mk	2.35.2	2.36.1 found by distro	0	Link	CVE-2021-3487	cpe:2.3:a:gnu:binutils:2.35.2:*:*:*:*:*:*:*
package/busybox/busybox.mk	1.33.0	1.33.1 found by distro	0	Link	N/A	cpe:2.3:a:busybox:busybox:1.33.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/cairo/cairo.mk	1.16.0	1.17.4 found by distro	0	Link	CVE-2019-6461 CVE-2019-6462 CVE-2020-35492	cpe:2.3:a:cairographics:cairo:1.16.0:*:*:*:*:*:*:*
package/cifs-utils/cifs-utils.mk	6.11	6.13 found by distro	0	Link	CVE-2021-20208	cpe:2.3:a:samba:cifs-utils:6.11:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/expat/expat.mk	2.2.10	2.4.1 found by distro	0	Link	CVE-2013-0340	cpe:2.3:a:libexpat_project:libexpat:2.2.10:*:*:*:*:*:*:*
package/fakeroot/fakeroot.mk	1.25.3	1.25.3 found by distro	0	Link	N/A	no verified CPE identifier
package/fontconfig/fontconfig.mk	2.13.1	2.13.93 found by distro	0	Link	N/A	cpe:2.3:a:fontconfig_project:fontconfig:2.13.1:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/freetype/freetype.mk	2.10.4	2.10.4 found by distro	0	Link	N/A	cpe:2.3:a:freetype:freetype:2.10.4:*:*:*:*:*:*:* CPE identifier unknown in CPE database

CPE identifiers

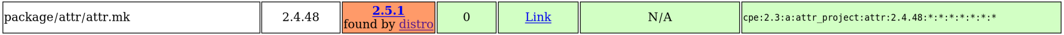
- By default
  - Buildroot generates a CPE identifier equal to: `cpe:2.3:a:<pkg>_project:<pkg>:<pkg-version>:*:*:*:*:*:*`
  - Sometimes doesn't match with how the software component is referenced in the NVD CPE dictionary
- Can be overridden on a per-package basis with:
  - `<pkg>_CPE_ID_PREFIX`
  - `<pkg>_CPE_ID_VENDOR`
  - `<pkg>_CPE_ID_PRODUCT`
  - `<pkg>_CPE_ID_VERSION`
  - `<pkg>_CPE_ID_UPDATE`
- The `pkg-stats` output indicates if the generated CPE identifier has been found in the CPE dictionary. If not found:
  - Incorrect CPE information in Buildroot
  - Incomplete CPE dictionary
- Many Buildroot packages already annotated with correct CPE ID information.

pkg-stats output details



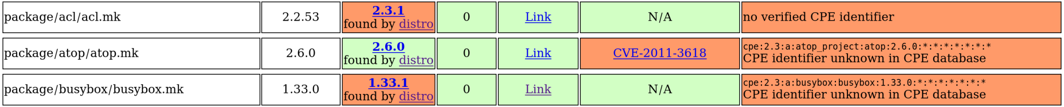
package/attr/attr.mk	2.4.48	**2.5.1** found by distro	0	Link	N/A	cpe:2.3:a:attr_project:attr:2.4.48:*:*:*:*:*:*:*
package/acl/acl.mk	2.2.53	**2.3.1** found by distro	0	Link	N/A	no verified CPE identifier
package/atop/atop.mk	2.6.0	**2.6.0** found by distro	0	Link	CVE-2011-3618	cpe:2.3:a:atop_project:atop:2.6.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/busybox/busybox.mk	1.33.0	**1.33.1** found by distro	0	Link	N/A	cpe:2.3:a:busybox:busybox:1.33.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database

pkg-stats output details



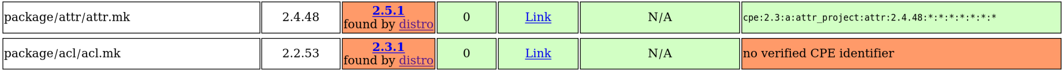
package/attr/attr.mk	2.4.48	2.5.1 found by distro	0	Link	N/A	cpe:2.3:a:attr_project:attr:2.4.48:*:*:*:*:*:*:*

- some <pkg>_CPE_ID_* variables defined → CPE information verified
- CPE identifier exists in the CPE dictionary
- no known CVEs



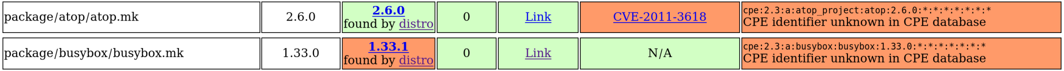
package/acl/acl.mk	2.2.53	2.3.1 found by distro	0	Link	N/A	no verified CPE identifier
package/atop/atop.mk	2.6.0	2.6.0 found by distro	0	Link	CVE-2011-3618	cpe:2.3:a:atop_project:atop:2.6.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/busybox/busybox.mk	1.33.0	1.33.1 found by distro	0	Link	N/A	cpe:2.3:a:busybox:busybox:1.33.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database

pkg-stats output details



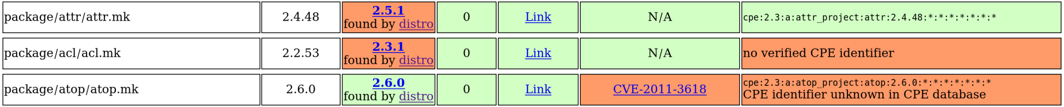
package/attr/attr.mk	2.4.48	**2.5.1** found by distro	0	Link	N/A	cpe:2.3:a:attr_project:attr:2.4.48:*:*:*:*:*:*:*
package/acl/acl.mk	2.2.53	**2.3.1** found by distro	0	Link	N/A	no verified CPE identifier

- no `<pkg>_CPE_ID_*` variable → don't know if the default CPE identifier is correct
- based on this default CPE identifier → no known CVE



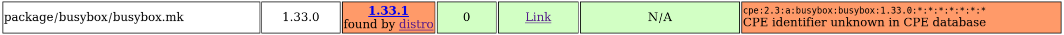
package/atop/atop.mk	2.6.0	**2.6.0** found by distro	0	Link	CVE-2011-3618	cpe:2.3:a:atop_project:atop:2.6.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/busybox/busybox.mk	1.33.0	**1.33.1** found by distro	0	Link	N/A	cpe:2.3:a:busybox:busybox:1.33.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database

pkg-stats output details



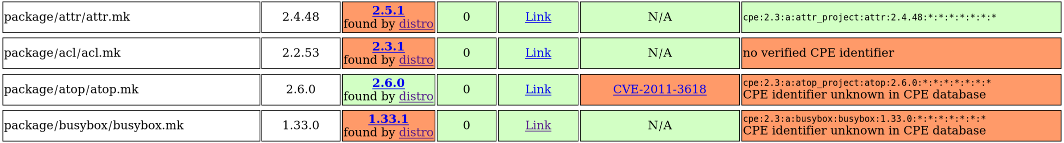
package/attr/attr.mk	2.4.48	**2.5.1** found by distro	0	Link	N/A	`cpe:2.3:a:attr_project:attr:2.4.48:*:*:*:*:*:*:*`
package/acl/acl.mk	2.2.53	**2.3.1** found by distro	0	Link	N/A	no verified CPE identifier
package/atop/atop.mk	2.6.0	**2.6.0** found by distro	0	Link	CVE-2011-3618	`cpe:2.3:a:atop_project:atop:2.6.0:*:*:*:*:*:*:*` CPE identifier unknown in CPE database

- some `<pkg>_CPE_ID_*` variables defined → CPE information verified
- no entry in CPE dictionary → version 2.6.0 not known by NVD
- CVE-2011-3618 applicable: NVD database indicates it applies to all versions.



package/busybox/busybox.mk	1.33.0	**1.33.1** found by distro	0	Link	N/A	`cpe:2.3:a:busybox:busybox:1.33.0:*:*:*:*:*:*:*` CPE identifier unknown in CPE database

pkg-stats output details



package/attr/attr.mk	2.4.48	2.5.1 found by distro	0	Link	N/A	cpe:2.3:a:attr_project:attr:2.4.48:*:*:*:*:*:*:*
package/acl/acl.mk	2.2.53	2.3.1 found by distro	0	Link	N/A	no verified CPE identifier
package/atop/atop.mk	2.6.0	2.6.0 found by distro	0	Link	CVE-2011-3618	cpe:2.3:a:atop_project:atop:2.6.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database
package/busybox/busybox.mk	1.33.0	1.33.1 found by distro	0	Link	N/A	cpe:2.3:a:busybox:busybox:1.33.0:*:*:*:*:*:*:* CPE identifier unknown in CPE database

- some `<pkg>_CPE_ID_*` variables defined → CPE information verified
- no entry in CPE dictionary → version 1.33.0 not known by NVD
- no known CVEs

Ignoring CVEs

- Sometimes a CVE is reported as applicable to particular version but should be ignored by Buildroot
- Typical reasons:
  - Buildroot has backported the security fix as a patch in `package/<pkg>/`
  - The security issue doesn't apply to the Buildroot configuration/usage of the package
- `<pkg>_IGNORE_CVES` can be used per package to ignore specific CVEs

package/bind/bind.mk

```
# Only applies to RHEL6.x with DNSSEC validation on
BIND_IGNORE_CVES = CVE-2017-3139
```

package/hostapd/hostapd.mk

```
# 0002-ASN.1-Validate-DigestAlgorithmIdentifier-parameters.patch
HOSTAPD_IGNORE_CVES += CVE-2021-30004
```

Limitations

- Packages with **custom versions** from Git (Linux, U-Boot, etc.) → Buildroot doesn't know how to match custom versions with well-known upstream releases.
- **CPE dictionary not complete** and/or **inaccuracies** in CVE reports
  - NVD maintainers open to contributions
  - Buildroot developers have successfully contributed to the CPE and CVE databases
- **Only** tracks security issues reported as CVEs
  - Some security issues not reported as CVEs
  - Proprietary/in-house software is regularly much worse from a security standpoint!

Conclusion

- Security vulnerability tracking has become important to keep devices updated
- NVD provides useful databases, in machine-parsable formats
- Buildroot `pkg-stats` is the entry point to use such databases in a Buildroot context
- Run `pkg-stats` in a cronjob and monitor the results
- If a package if affected by a CVE
  - See if a version upgrade is necessary
  - Or backport the security fix + add `<pkg>_IGNORE_CVES`
  - Contribute the result to upstream Buildroot!

Questions? Suggestions? Comments?

Thomas Petazzoni

thomas.petazzoni@bootlin.com