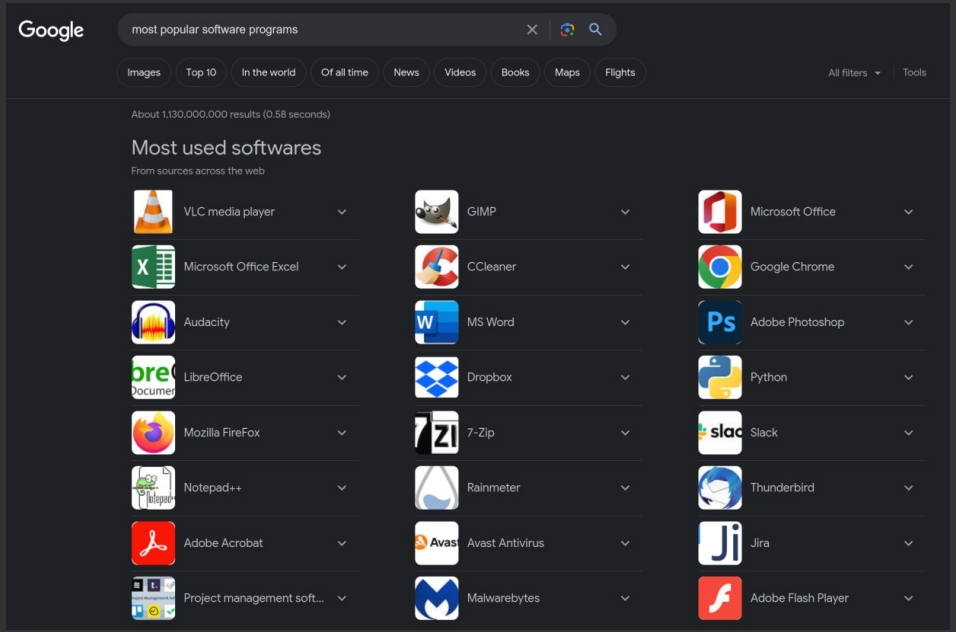
>>> Predict security attacks in FOSS

>>> Why you want it and how to do it

Name: Carlos E. Budde
Inst: University of Trento, Italy
Date: 10th November 2023

ProSVED

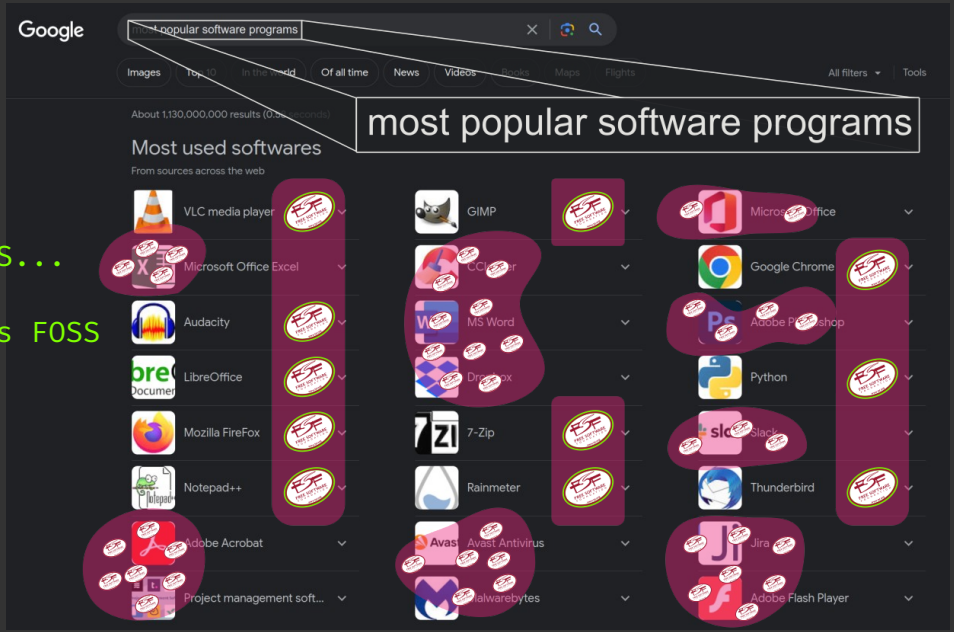
AssureMOSS


Google
most popular software programs
Images
Top 10
In the world
Of all time
News
Videos
Books
Maps
Flights
All filters
Tools
About 1,130,000,000 results (0.58 seconds)
Most used softwares
From sources across the web
VLC media player
GIMP
Microsoft Office
Microsoft Office Excel
CCleaner
Google Chrome
Audacity
MS Word
Adobe Photoshop
LibreOffice
Dropbox
Python
Mozilla FireFox
7-Zip
Slack
Notepad++
Rainmeter
Thunderbird
Adobe Acrobat
Avast Antivirus
Jira
Project management soft...
Malwarebytes
Adobe Flash Player


Google
popular software programs
Images
Top 10
In the world
Of all time
News
Videos
Books
Maps
Flights
All filters
Tools
About 1,130,000,000 results (0.53 seconds)
most popular software programs
Most used softwares
From sources across the web
VLC media player
Microsoft Office Excel
Audacity
LibreOffice
Mozilla FireFox
Notepad++
Adobe Acrobat
Project management soft...
GIMP
CCleaner
MS Word
Dropbox
7-Zip
Rainmeter
Avast Antivirus
Malwarebytes
Microsoft Office
Google Chrome
Adobe Photoshop
Python
Slack
Thunderbird
Jira
Adobe Flash Player

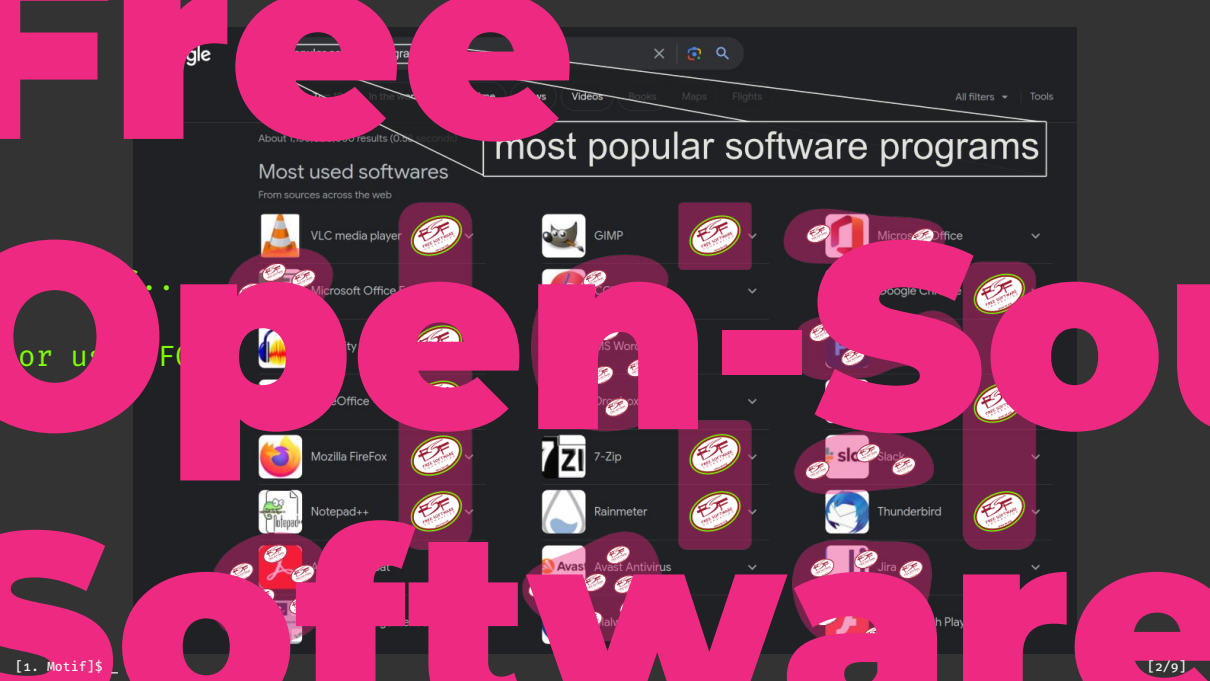
is FOSS...

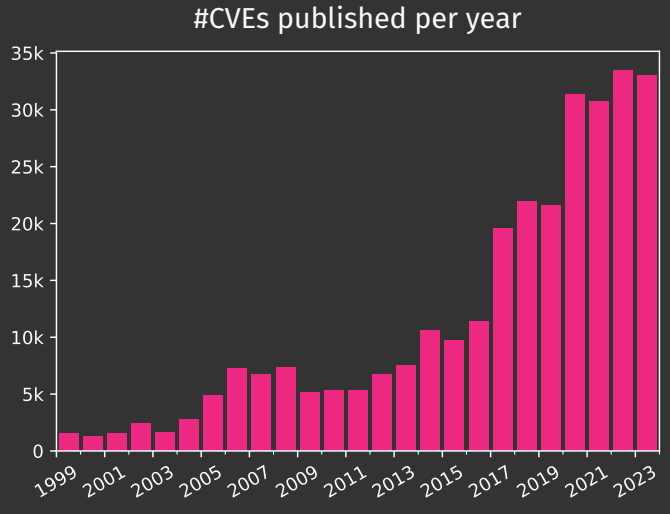

Google
popular software programs
Images
Of all time
News
Videos
Books
Maps
Flights
All filters
Tools
About 1,130,000,000 results
most popular software programs
Most used softwares
From sources across the web
VLC media player
GIMP
Microsoft Office
Microsoft Office Excel
CCleaner
Google Chrome
Audacity
MS Word
Adobe Photoshop
LibreOffice
Dropbox
Python
Mozilla FireFox
7-Zip
Slack
Notepad++
Rainmeter
Thunderbird
Adobe Acrobat
Avast Antivirus
Jira
Project management soft...
Malwarebytes
Adobe Flash Player



is FOSS...

or uses FOSS


Free
most popular software programs
Open-Source
Software
Most used softwares
From sources across the web
VLC media player
GIMP
Mozilla FireFox
7-Zip
Notepad++
Rainmeter
Thunderbird
Avast Antivirus
Videos
Books
Maps
Flights
All filters
Tools
[1. Motif]$ _
[2/9]

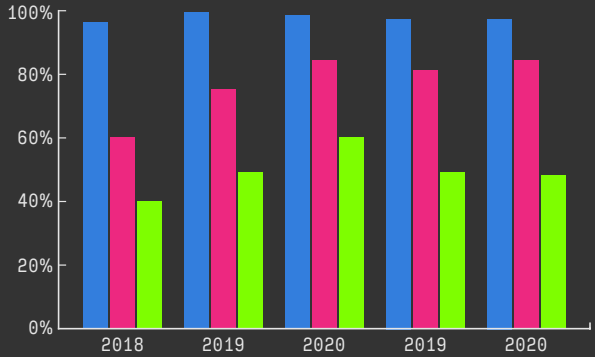


NVD

MITRE

Source: https://cve.mitre.org/data/downloads/allitems.csv.Z

Open-source software and vulnerabilities



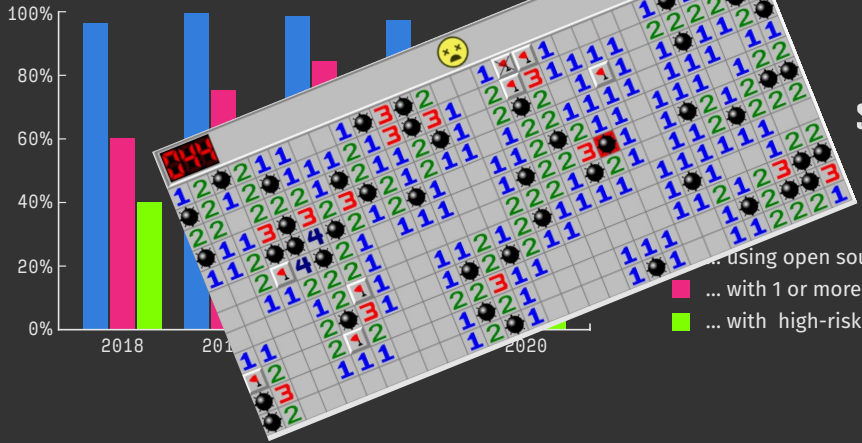
SYNOPSYS®

Codebases ...

- ... using open source software
- ... with 1 or more vulnerabilities
- ... with high-risk vulnerabilities

Source: https://www.synopsys.com/software-integrity/engage/ossra/rep-ossra-2023-pdf

Open-source software and vulnerabilities



Source: https://www.synopsys.com/software-integrity/engage/ossra/rep-ossra-2023-pdf

>>> Vulnerabilities in dependency tree

```
$ mvn dependency:tree
[INFO] Scanning for projects...
⋮
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] |  +- io.netty:netty-transport-native-unix-common:jar:4.1.86.Final:compile
[INFO] |  \- io.netty:netty-transport-classes-kqueue:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-transport-native-epoll:jar:4.1.86.Final:provided
[INFO] |  \- io.netty:netty-transport-classes-epoll:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-common:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-codec:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-buffer:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-transport:jar:4.1.86.Final:compile
⋮
```

>>> Vulnerabilities in dependency tree

```
$ mvn dependency:tree
[INFO] Scanning for projects...
⋮
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] | +- io.netty:netty-transport-native-unix-common:jar:4.1.86.Final:compile
[INFO] | \- io.netty:netty-transport-classes-kqueue:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-transport-native-epoll:jar:4.1.86.Final:provided
[INFO] | \- io.netty:netty-transport-classes-epoll:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-common:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-codec:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-buffer:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-transport:jar:4.1.86.Final:compile
⋮
```

Dependency tree of Redisson v3.19.0

>>> Vulnerabilities in dependency tree

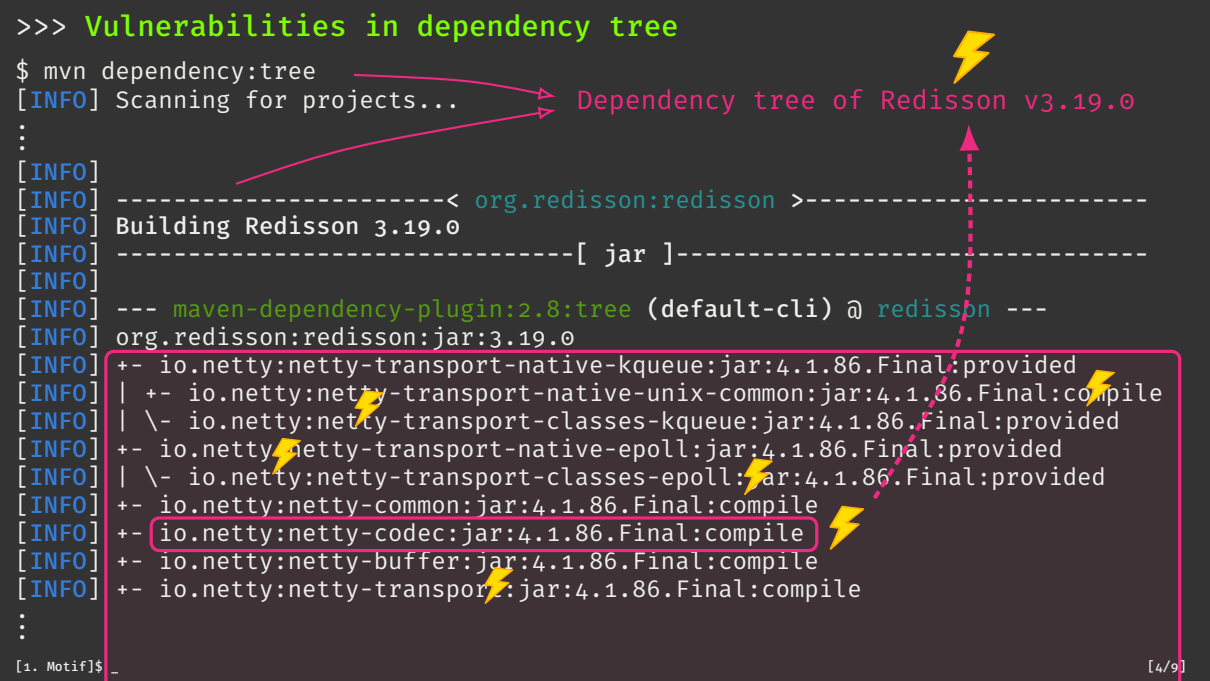
```
$ mvn dependency:tree
[INFO] Scanning for projects...
⋮
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] |  +- io.netty:netty-transport-native-unix-common:jar:4.1.86.Final:compile
[INFO] |  \- io.netty:netty-transport-classes-kqueue:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-transport-native-epoll:jar:4.1.86.Final:provided
[INFO] |  \- io.netty:netty-transport-classes-epoll:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-common:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-codec:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-buffer:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-transport:jar:4.1.86.Final:compile
⋮
```

Dependency tree of Redisson v3.19.0

>>> Vulnerabilities in dependency tree

```
$ mvn dependency:tree
[INFO] Scanning for projects...
⋮
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] |  +- io.netty:netty-transport-native-unix-common:jar:4.1.86.Final:compile
[INFO] |  \- io.netty:netty-transport-classes-kqueue:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-transport-native-epoll:jar:4.1.86.Final:provided
[INFO] |  \- io.netty:netty-transport-classes-epoll:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-common:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-codec:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-buffer:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-transport:jar:4.1.86.Final:compile
⋮
```

Dependency tree of Redisson v3.19.0


>>> Vulnerabilities in dependency tree
$ mvn dependency:tree
[INFO] Scanning for projects...
Dependency tree of Redisson v3.19.0
[INFO]
[INFO] ----------------------< org.redisson:redisson >-----------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[jar]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] | +- io.netty:netty-transport-native-unix-common:jar:4.1.86.Final:compile
[INFO] | \- io.netty:netty-transport-classes-kqueue:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-transport-native-epoll:jar:4.1.86.Final:provided
[INFO] | \- io.netty:netty-transport-classes-epoll:jar:4.1.86.Final:provided
[INFO] +- io.netty:netty-common:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-codec:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-buffer:jar:4.1.86.Final:compile
[INFO] +- io.netty:netty-transport:jar:4.1.86.Final:compile
[1. Motif]$ _
[4/9]

>>> Vulnerabilities in dependency tree

```
$ mvn dependency:tree
[INFO] Scanning for projects...
:
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] | +- io.netty:                                          on:jar:4.1.86.Final:compile
[INFO] | \- io.netty:                                          ar:4.1.86.Final:provided
[INFO] +- io.netty:ne                                          .1.86.Final:provided
[INFO] | \- io.netty:                                          r:4.1.86.Final:provided
[INFO] +- io.netty:ne                                          ile
[INFO] +- io.netty:ne                                          le
[INFO] +- io.netty:ne                                          lle
[INFO] +- io.netty:ne                                          ompile
:
```

Dependency tree of Redisson v3.19.0

>>> Vulnerabilities in dependency tree

```
$ mvn dependency:tree
[INFO] Scanning for projects...
:
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] |  +- io.netty:                                          on:jar:4.1.86.Final:compile
[INFO] |  \- io.netty:                                          ar:4.1.86.Final:provided
[INFO] +- io.netty:ne                                           .1.86.Final:provided
[INFO] |  \- io.netty:                                          r:4.1.86.Final:provided
[INFO] +- io.netty:ne                                           ile
[INFO] +- io.netty:ne                                           le
[INFO] +- io.netty:ne                                           lle
[INFO] +- io.netty:ne                                           ompile
:
```

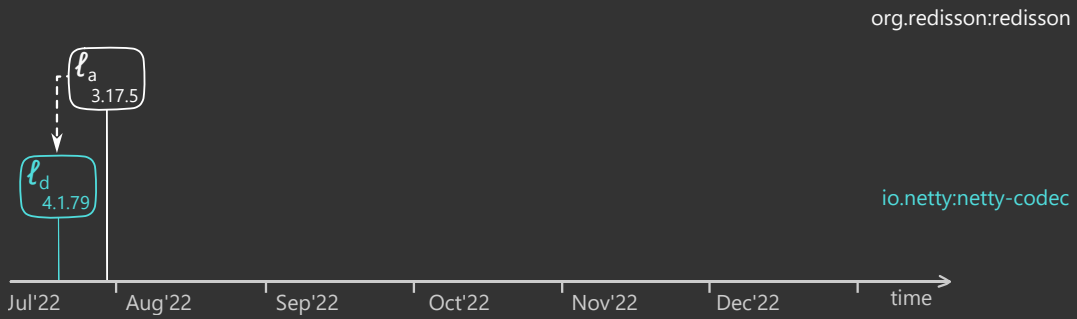
Dependency tree of Redisson v3.19.0

>>> Vulnerabilities in dependency tree

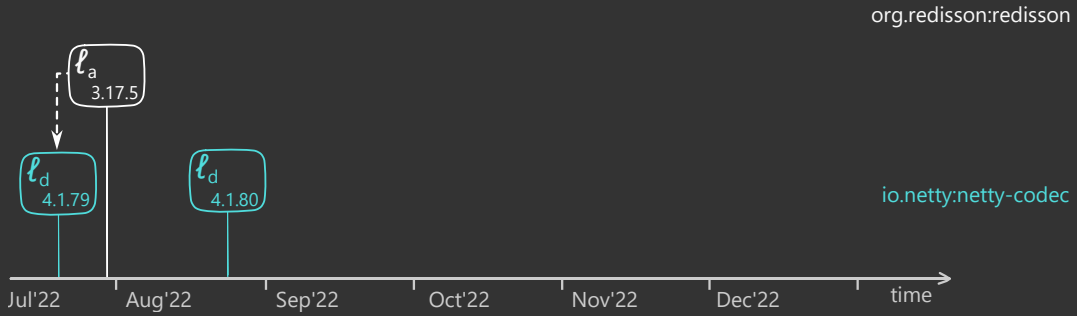
```
$ mvn dependency:tree
[INFO] Scanning for projects...
:
[INFO]
[INFO] ------------------------< org.redisson:redisson >-------------------------
[INFO] Building Redisson 3.19.0
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ redisson ---
[INFO] org.redisson:redisson:jar:3.19.0
[INFO] +- io.netty:netty-transport-native-kqueue:jar:4.1.86.Final:provided
[INFO] | +- io.netty:                                    on:jar:4.1.86.Final:compile
[INFO] | \- io.netty:                                    ar:4.1.86.Final:provided
[INFO] +- io.netty:ne                                    .1.86.Final:provided
[INFO] | \- io.netty:                                    r:4.1.86.Final:provided
[INFO] +- io.netty:ne                                    ile
[INFO] +- io.netty:ne                                    le
[INFO] +- io.netty:ne                                    lle
[INFO] +- io.netty:ne                                    ompile
:
```

Dependency tree of Redisson v3.19.0

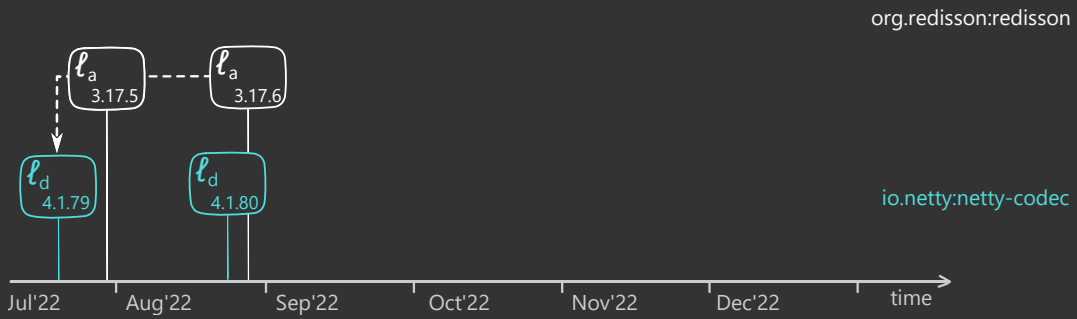
>>> Software's vulnerable lifecycle



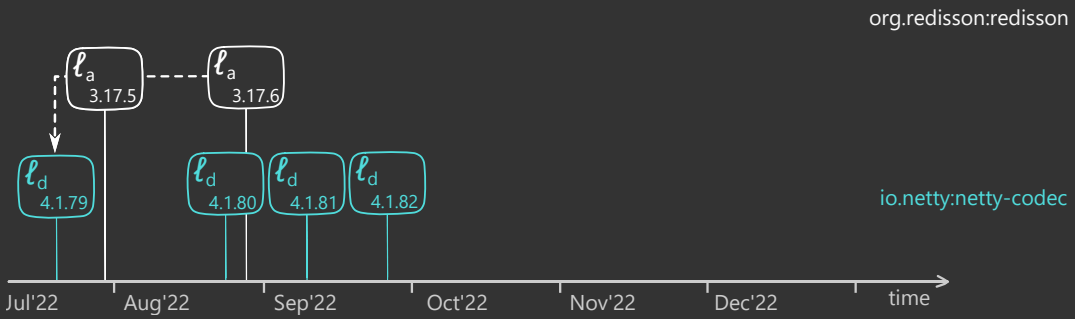
>>> Software's vulnerable lifecycle



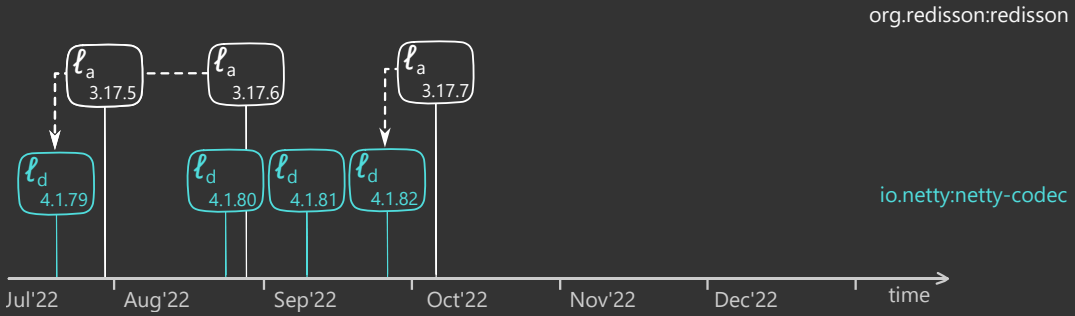
>>> Software's vulnerable lifecycle



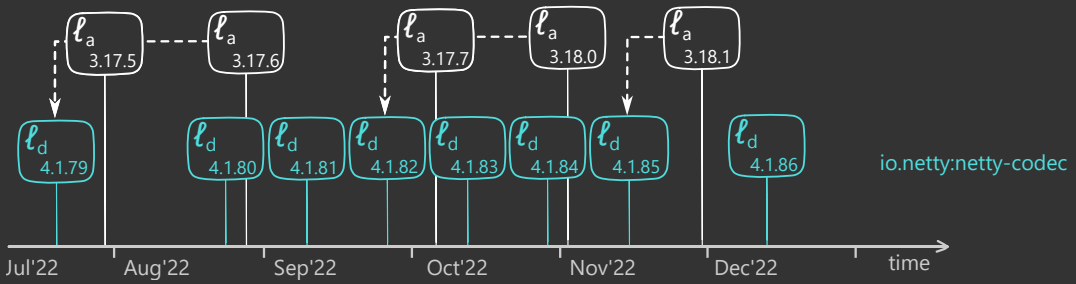
>>> Software's vulnerable lifecycle



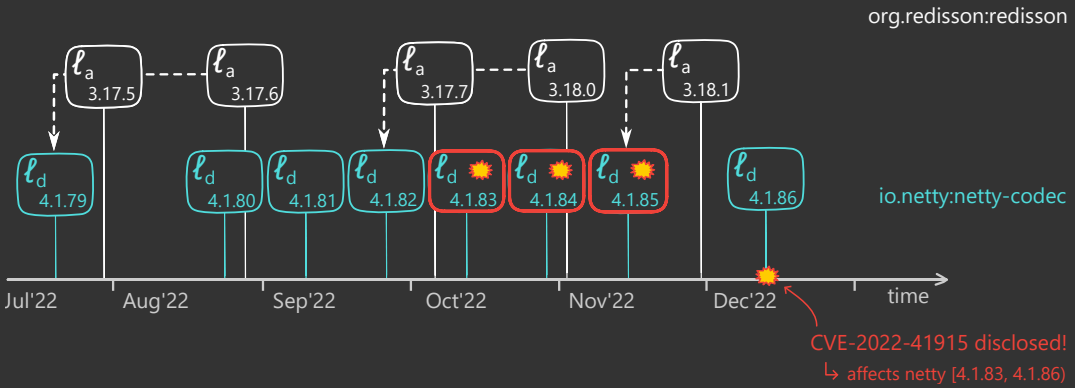
>>> Software's vulnerable lifecycle



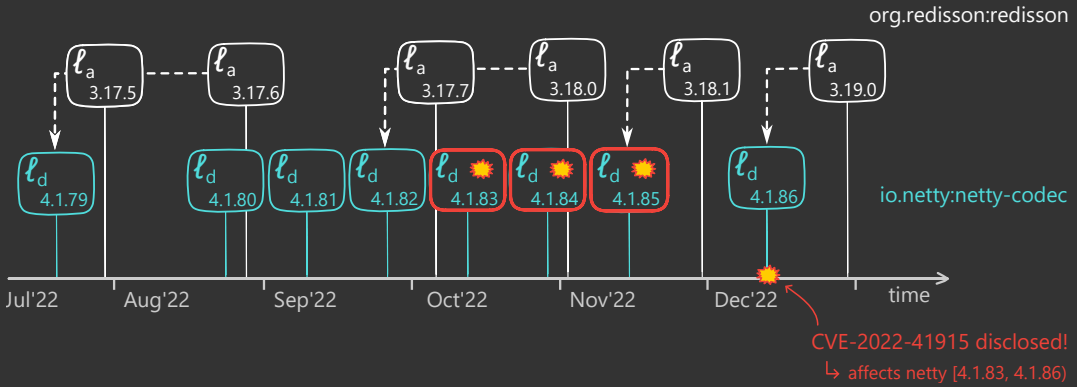
>>> Software's vulnerable lifecycle



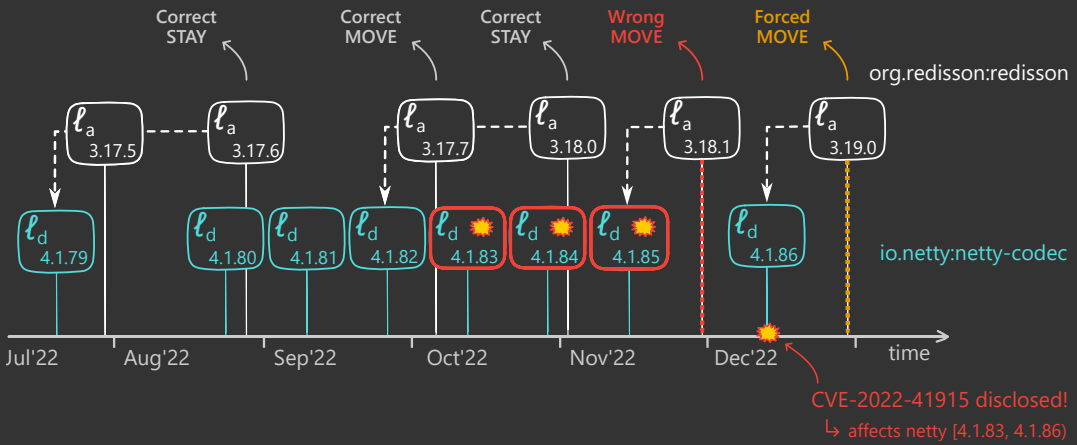
>>> Software's vulnerable lifecycle



>>> Software's vulnerable lifecycle

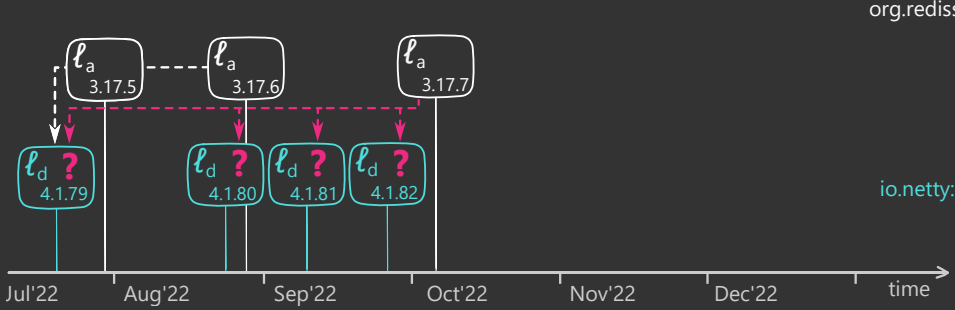


>>> Software's vulnerable lifecycle

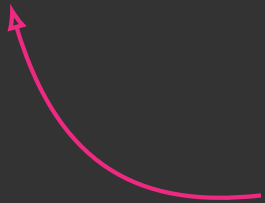


>>> Software's vulnerable lifecycle

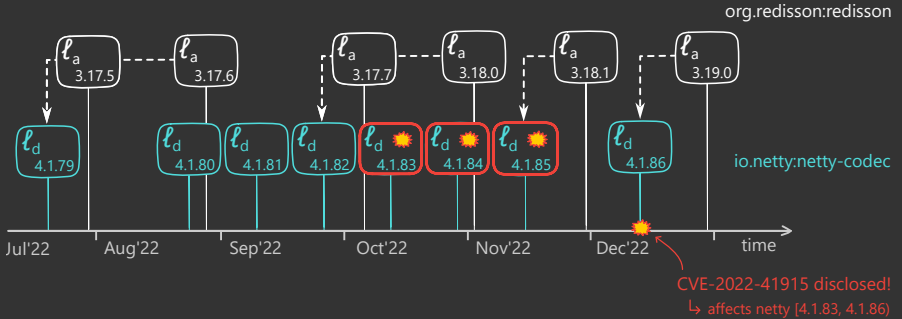
Is there a **best time** to update?



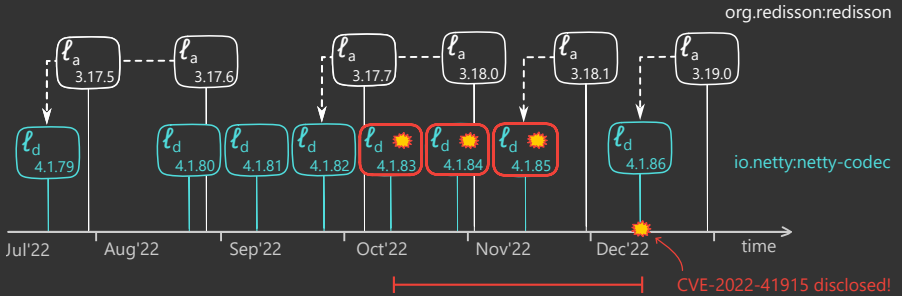
>>> Idea: fit CVE *disclosure time*



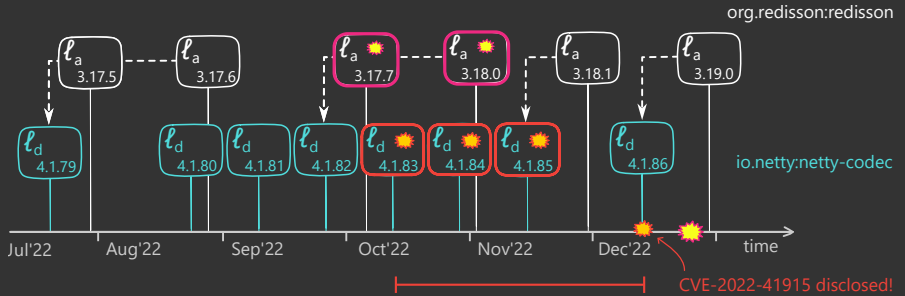
>>> Idea: fit CVE *disclosure time*



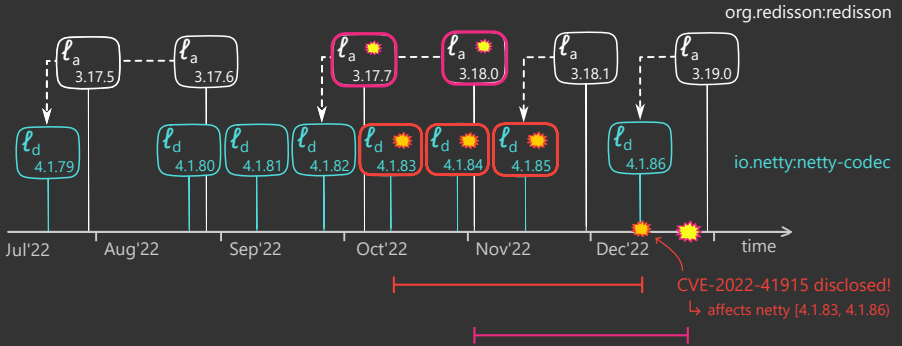
>>> Idea: fit CVE *disclosure time*



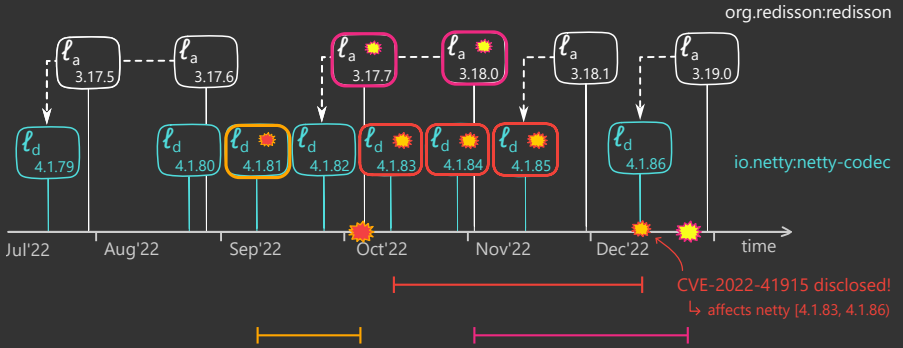
>>> Idea: fit CVE *disclosure time*



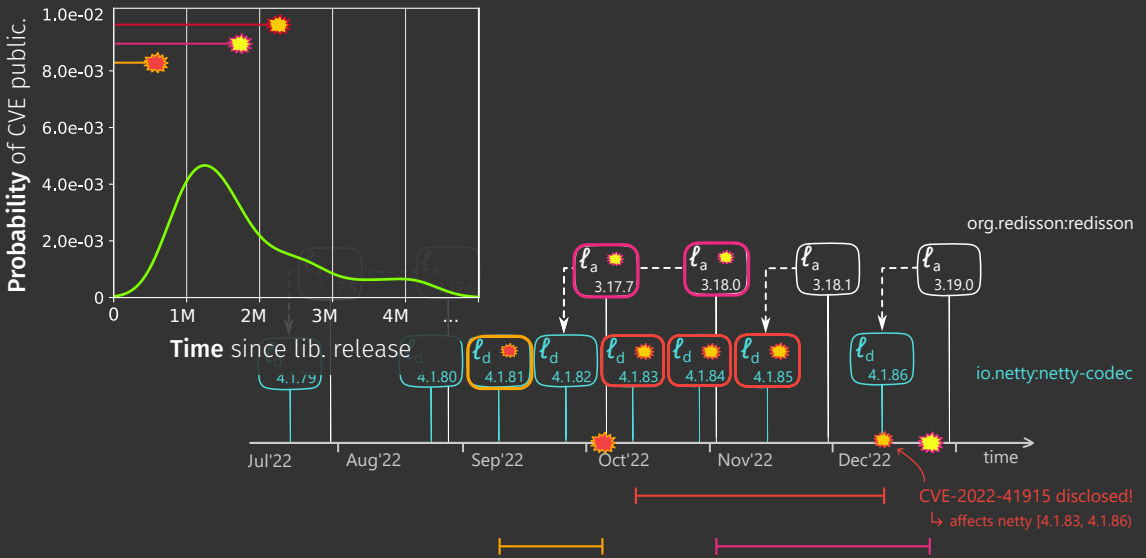
>>> Idea: fit CVE *disclosure time*



>>> Idea: fit CVE *disclosure time*



>>> Idea: fit CVE *disclosure time*



>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from

>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

* Not every vulnerability (or *library*) is equivalent

>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

* Not every vulnerability (or *library*) is equivalent
  - Partition software libraries per type

>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

* Not every vulnerability (or *library*) is equivalent
  - Partition software libraries per type

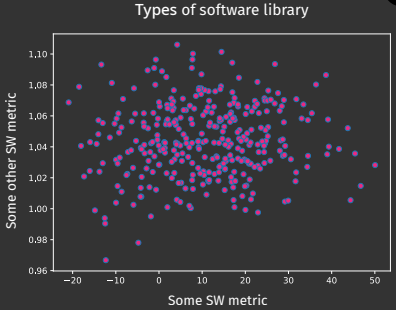
* Software features for classification
  that are relevant for security

>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

* Not every vulnerability (or *library*) is equivalent
  - Partition software libraries per type

* Software features for classification that are relevant for security

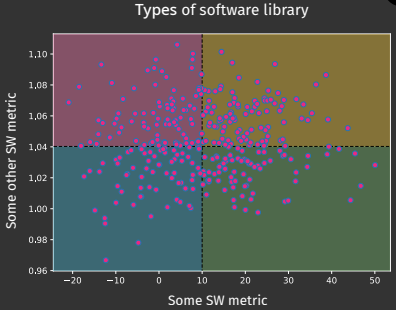


>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

* Not every vulnerability (or *library*) is equivalent
  - Partition software libraries per type

* Software features for classification that are relevant for security

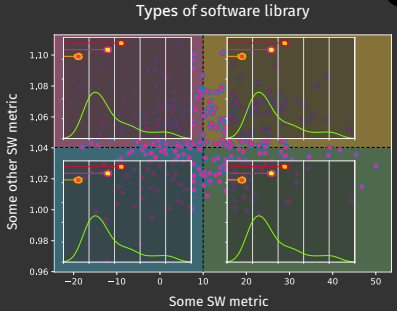


>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

* Not every vulnerability (or *library*) is equivalent
  - Partition software libraries per type

* Software features for classification that are relevant for security



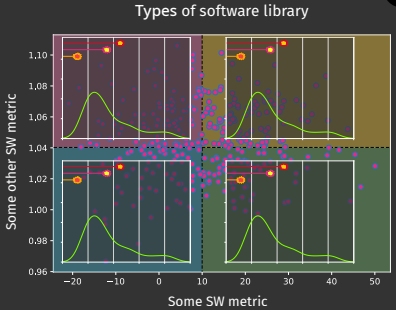
>>> But:

* Vulnerabilities are rare events ⇒ very few to fit from
  - Aggregate vulnerabilities from many libraries

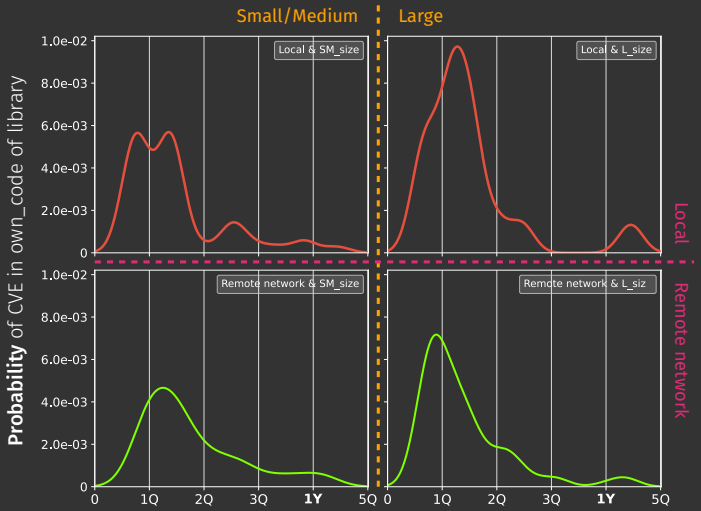
* Not every vulnerability (or *library*) is equivalent
  - Partition software libraries per type

* Software features for classification that are relevant for security

Features used to partition data, not to predict vulnerabilities



>>> Preliminary outcomes



>>> Predict security attacks in FOSS
>>> Why you want it and how to do it

Name: Carlos E. Budde†
Inst: University of Trento, Italy

Ethical security survey
—
Vrije Universiteit Amsterdam

https://vuass.eu.qualtrics.com/jfe/form/SV_cFSKOHjHZnaH2Si

ProSVED

AssureMOSS

†carlosesteban.budde@unitn.it