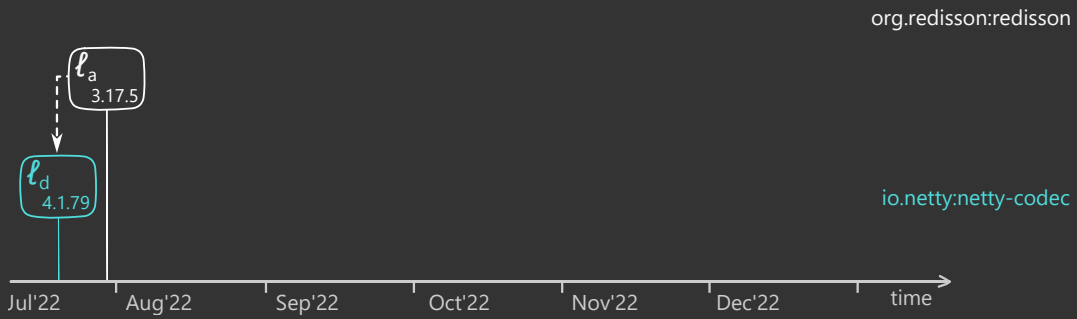
>>> Predict security vulnerabilities in FOSS

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

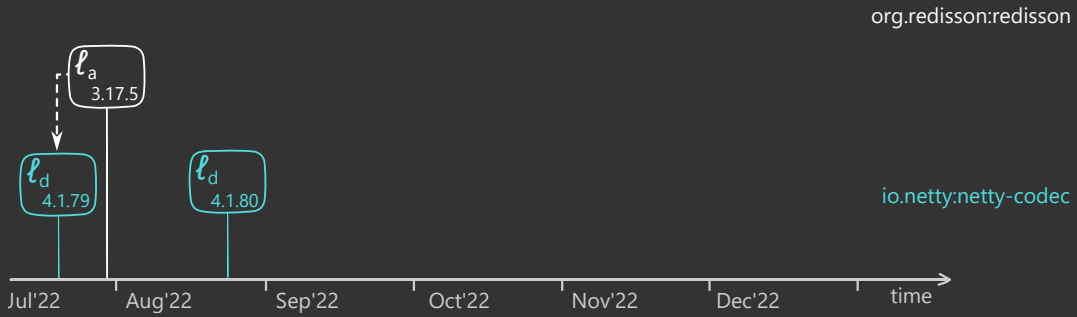
Name: Carlos E. Budde
Inst: Università di Trento, Italy
Date: 3rd November 2023

ProSVED

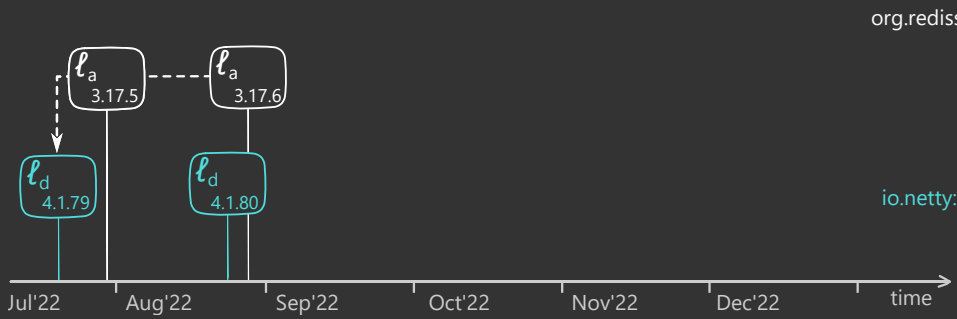
>>> Software's vulnerable lifecycle



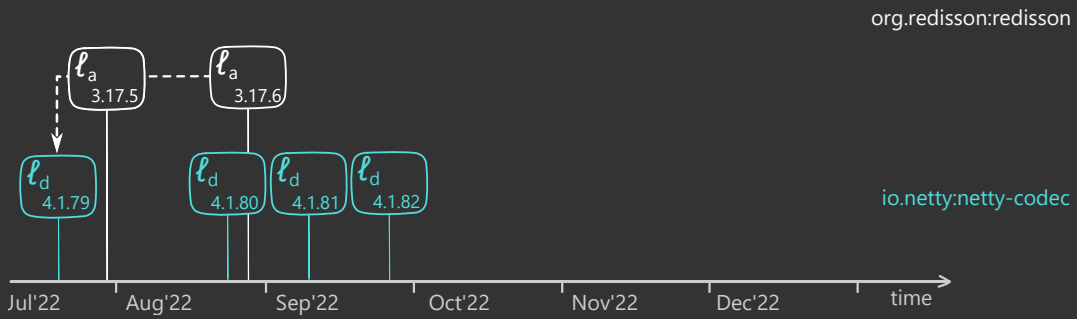
>>> Software's vulnerable lifecycle



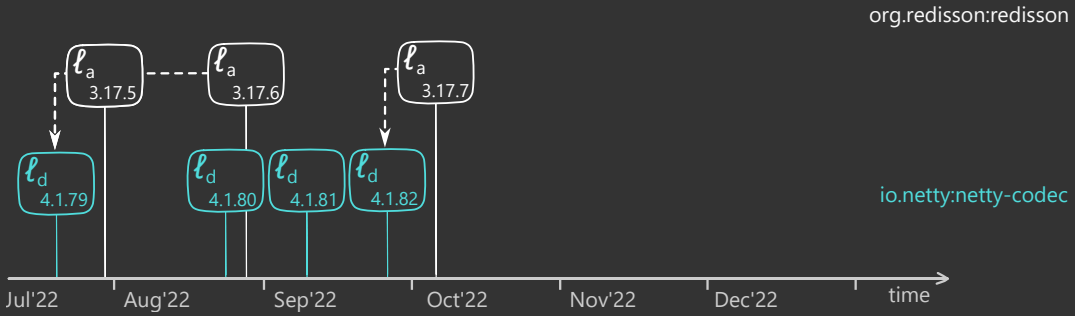
>>> Software's vulnerable lifecycle



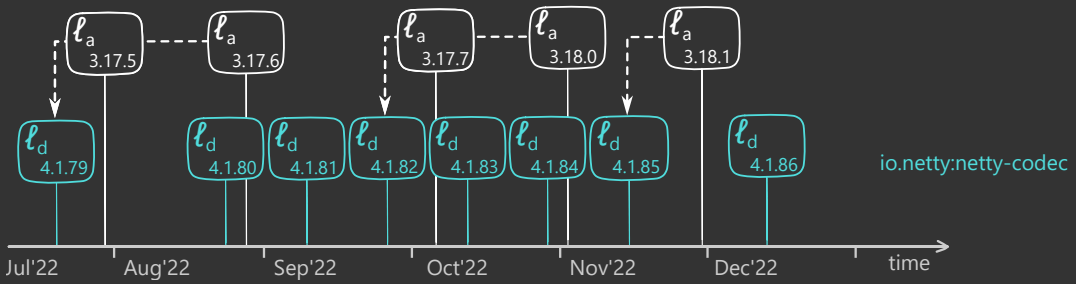
>>> Software's vulnerable lifecycle



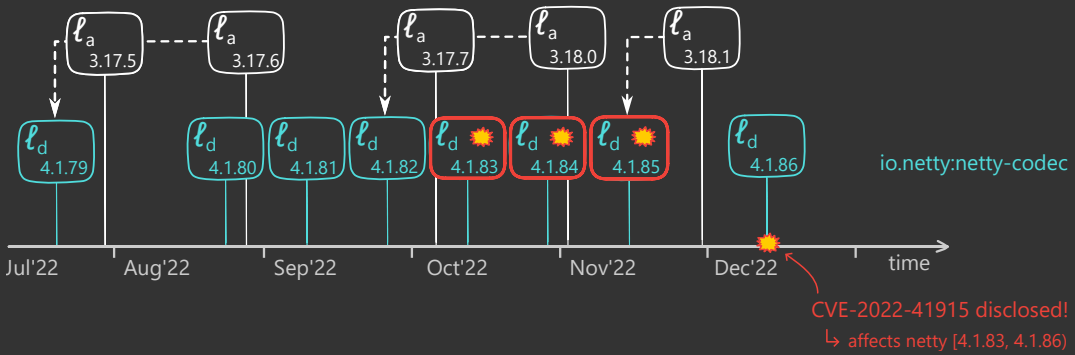
>>> Software's vulnerable lifecycle



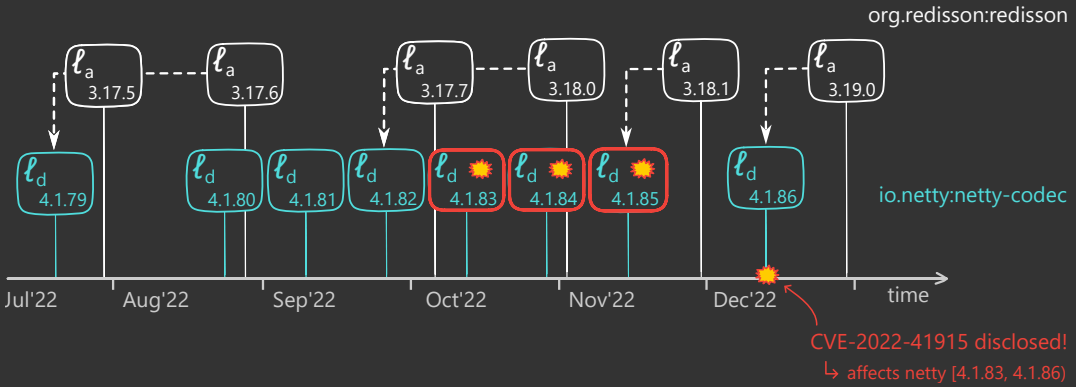
>>> Software's vulnerable lifecycle



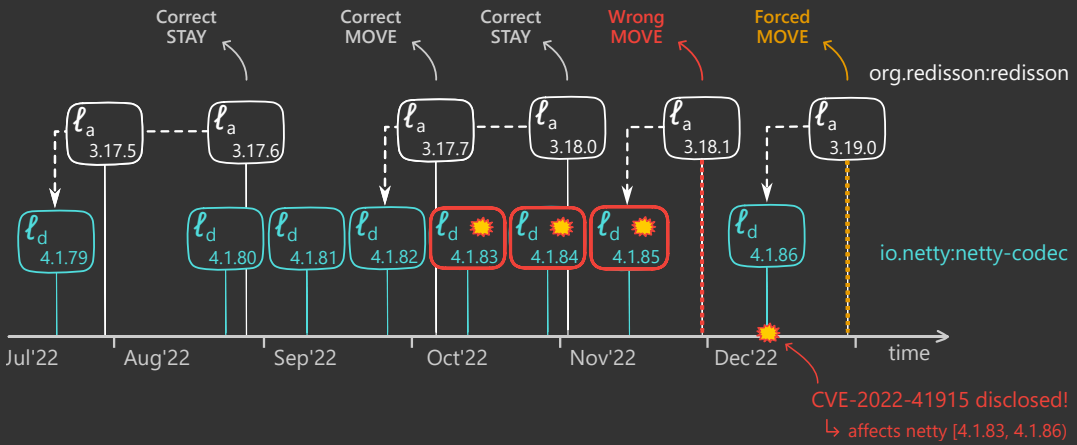
>>> Software's vulnerable lifecycle



>>> Software's vulnerable lifecycle

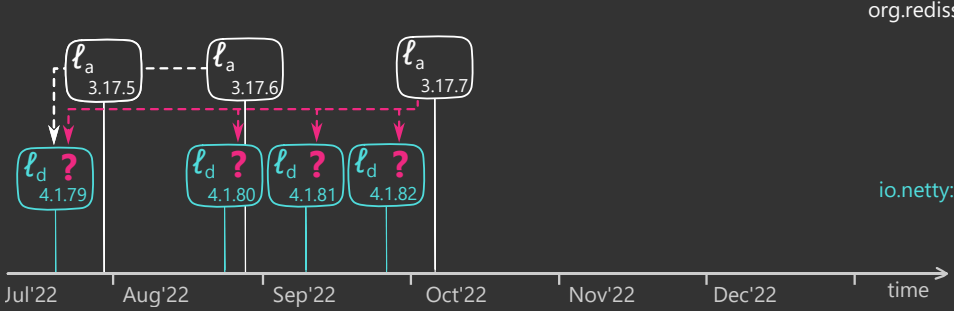


>>> Software's vulnerable lifecycle



>>> Software's vulnerable lifecycle

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



>>> Security vs. safety

>>> Security vs. safety

* Events are catastrophic
  - Vulnerability exploitation == death

>>> Security vs. safety

* Events are catastrophic
  - Vulnerability exploitation == death

* Events are rare
  - Very few files in very few libraries are vulnerable

>>> Security vs. safety

* Events are catastrophic
  - Vulnerability exploitation == death

* Events are rare
  - Very few files in very few libraries are vulnerable

* No good health indicators
  - Vulnerability exposed ⇒ insta kill

>>> Security vs. safety

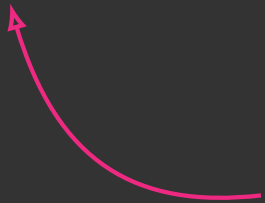
* Events are catastrophic
  - Vulnerability exploitation == death

* Events are rare
  - Very few files in very few libraries are vulnerable

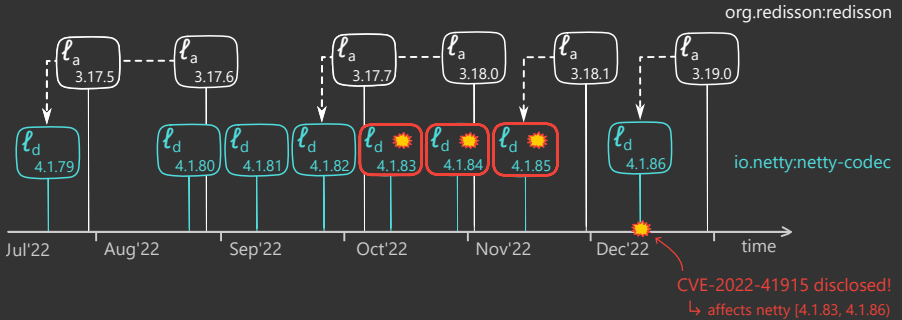
* No good health indicators
  - Vulnerability exposed ⇒ insta kill

Can we bridge the gap to use PdM for security?

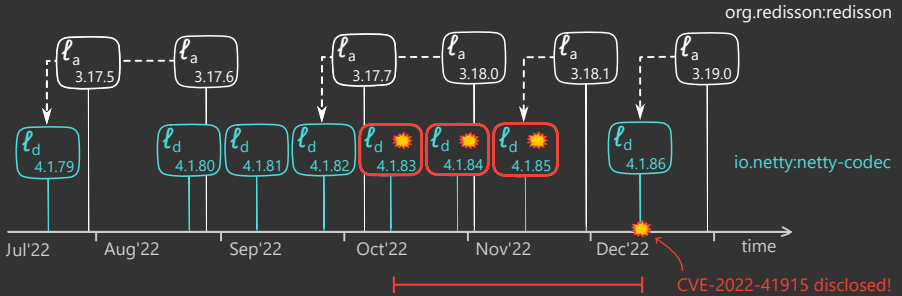
>>> Idea: fit CVE *disclosure time*



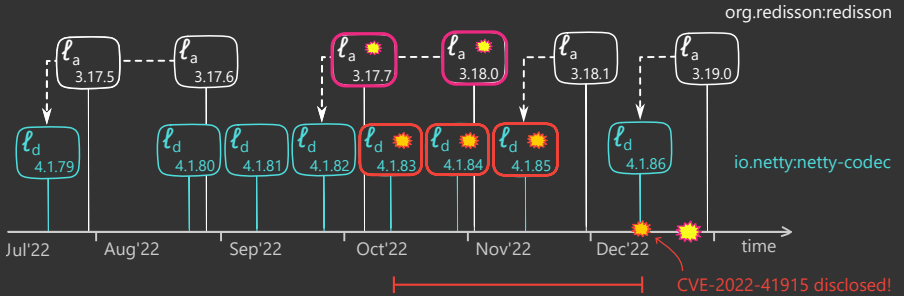
>>> Idea: fit CVE *disclosure time*



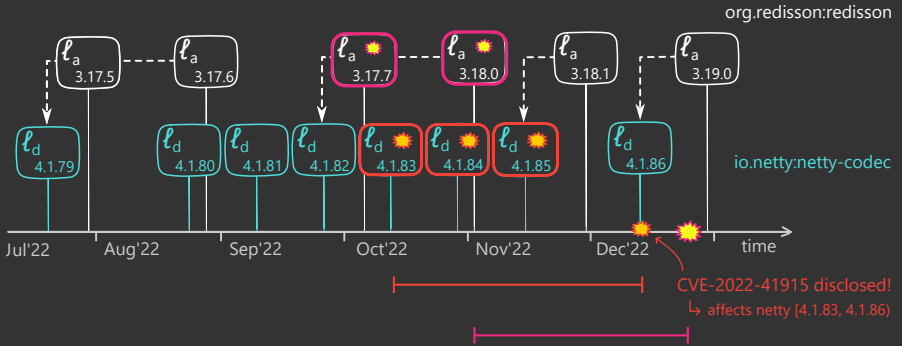
>>> Idea: fit CVE *disclosure time*



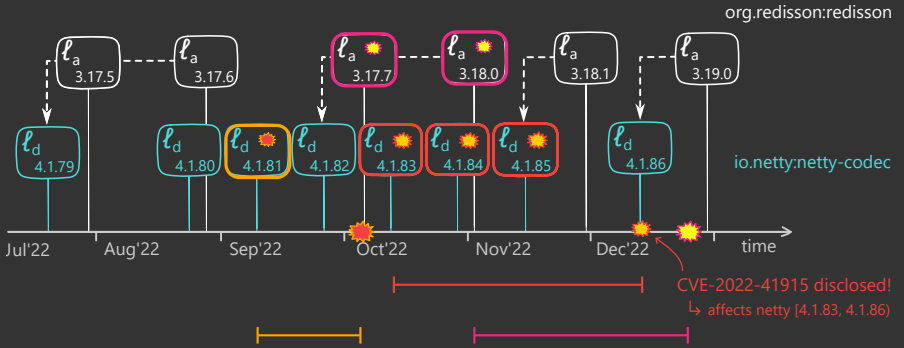
>>> Idea: fit CVE *disclosure time*



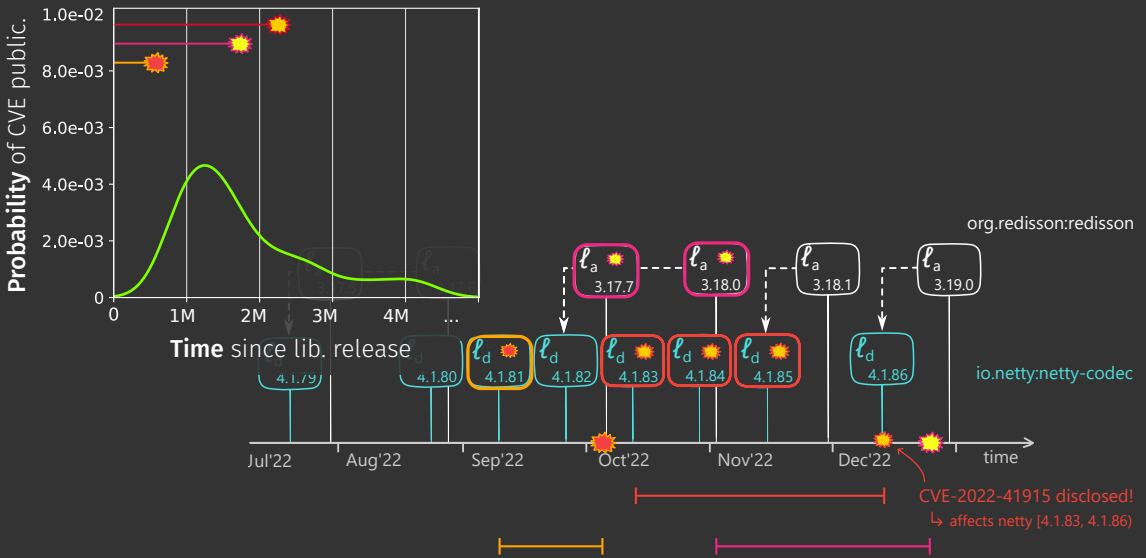
>>> Idea: fit CVE *disclosure time*



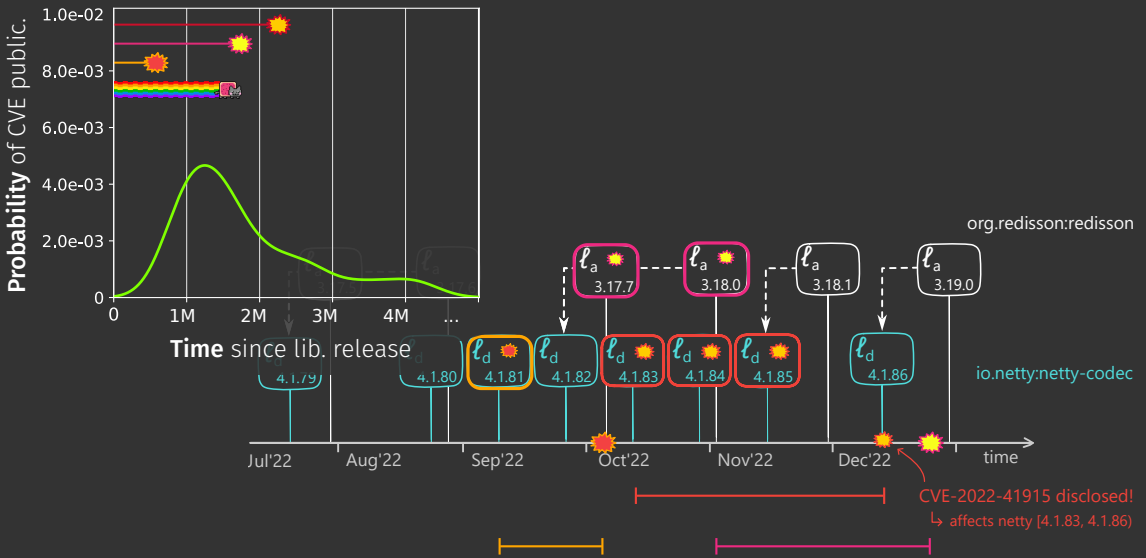
>>> Idea: fit CVE *disclosure time*



>>> Idea: fit CVE *disclosure time*



>>> 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

* 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

>>> 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

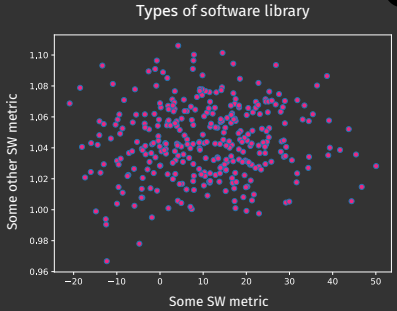
* Software features for classification
  that are relevant for security

>>> 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

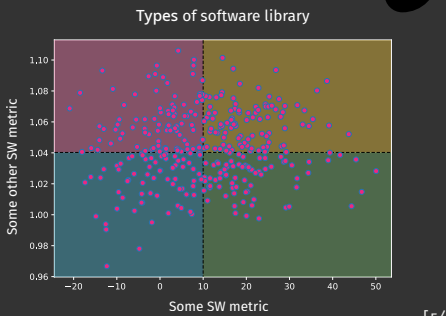


>>> But:

* 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

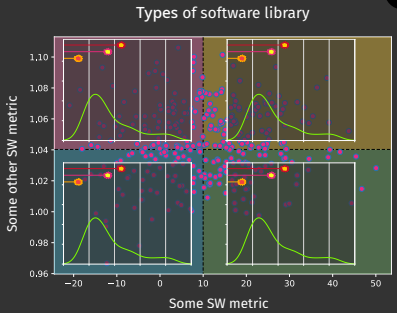


>>> But:

* 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

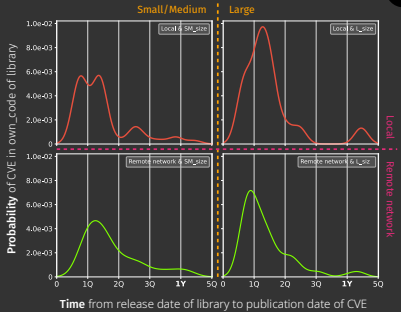


>>> But:

* 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**



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

Name: Carlos E. Budde[†]
Inst: Università di Trento, Italy

ProSVED

[†]carlosesteban.budde@unitn.it