Confusing Value with Enumeration: Studying the Use of CVEs in Academia

Moritz Schloegel [1], Daniel Klischies [2], Simon Koch [3], David Klein [3], Lukas Gerlach [1], Malte Wessels [3], Leon Trampert [1], Martin Johns [3], Mathy Vanhoef [4], Michael Schwarz [1], Thorsten Holz [1], Jo Van Bulck [4]

[1] CISPA Helmholtz Center for Information Security
[2] Ruhr University Bochum
[3] TU Braunschweig
[4] DistriNet, KU Leuven

USENIX Security 2025

Distinguished Paper

Do **you** know what a CVE is?

A **Common Vulnerabilities and Enumeration (CVE) ID** is a unique identifier assigned to a vulnerability

Two examples: **CVE-2014-0160** == Heartbleed

CVE-2017-5754 == Meltdown

A CVE ID == identifier? **But** ..

A CVE ID == identifier? **But** ..

*"[We] identified 19 [bugs] and obtained **11 new CVEs**."*

- abstract of some USENIX Security paper

A CVE ID == identifier? **But** ..

*"[We] identified 19 [bugs] and obtained **11 new CVEs**."*

- abstract of some USENIX Security paper

*"For 15 of [the bugs], the Chrome team assigned a CVE, **acknowledging the impact** of our results."*

- abstract of some ACM CCS paper

A CVE ID == identifier? **But ..**

*"[We] identified 19 [bugs] and obtained **11 new CVEs**."*

- abstract of some USENIX Security paper

*"For 15 of [the bugs], the Chrome team assigned a CVE, **acknowledging the impact** of our results."*

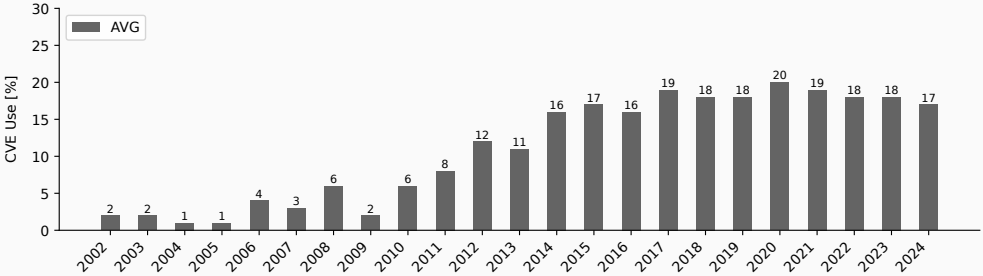
- abstract of some ACM CCS paper

.. also used as a proxy for impact!

1. How widespread is the **use** of CVEs?
2. What happened to the underlying **bugs**?
3. What does the **community** think?

Have **you** used CVEs in a paper?

1 Quantitative Analysis – General Use of CVEs



Average percentage of papers that mention one or more CVE IDs across

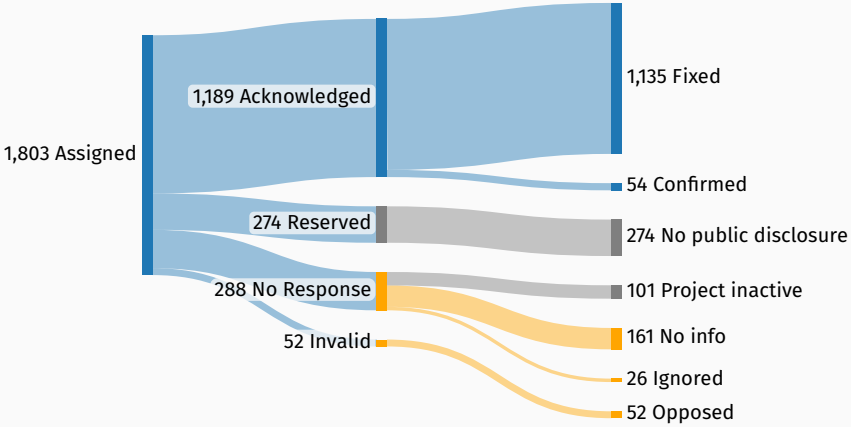
USENIX Security, IEEE S&P, ACM CCS, ISOC NDSS

Have **you** obtained CVEs for a paper?

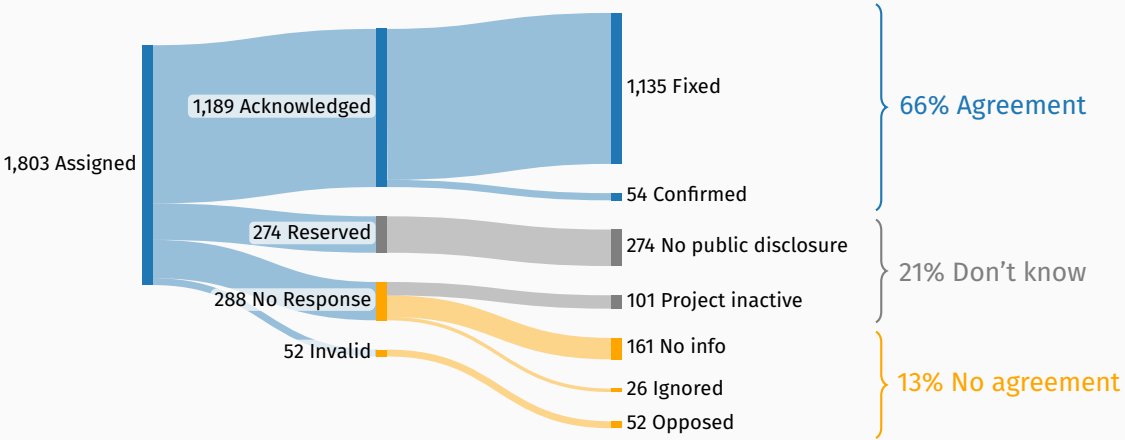
2 Qualitative Analysis – Outcome Classification

- Identified papers from 2020–2024 that **claimed** CVEs
- Extracted **1,803** CVEs claimed across **304** papers
- Analyzed the **outcomes** of the underlying bugs

2 Qualitative Analysis – Outcome Classification



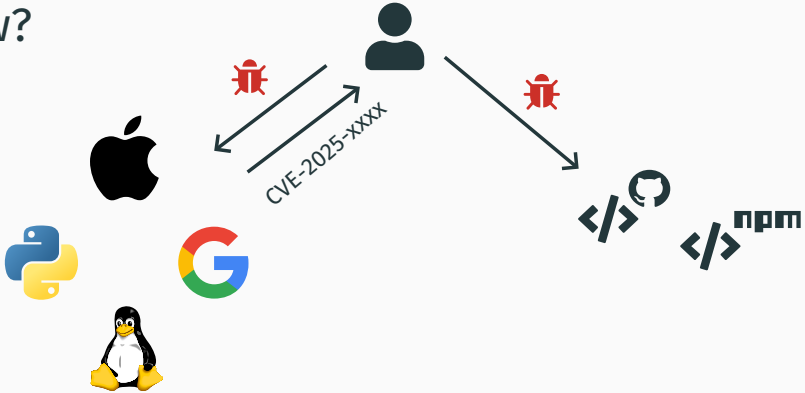
2 Qualitative Analysis – Outcome Classification



How?

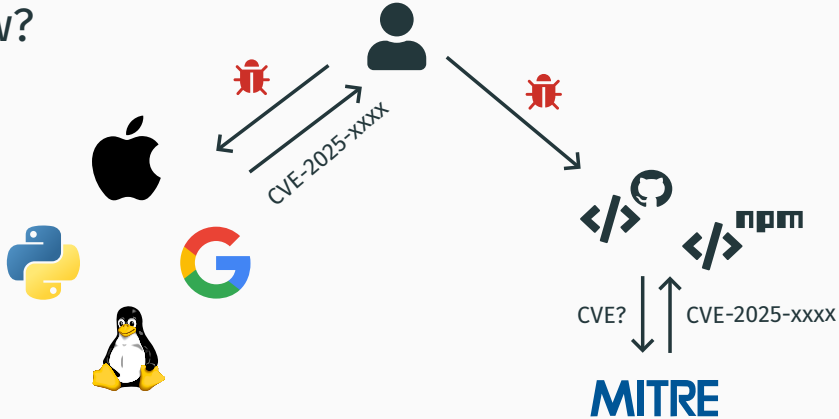
CVE Numbering Authorities (CNAs)

How?



CVE Numbering Authorities (CNAs)

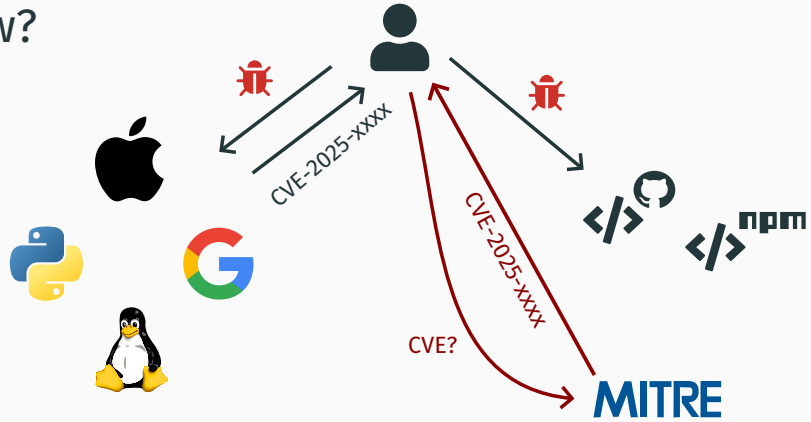
How?



CVE Numbering Authorities (CNAs)

CNAs of **Last Resort** (CNA-LRs)

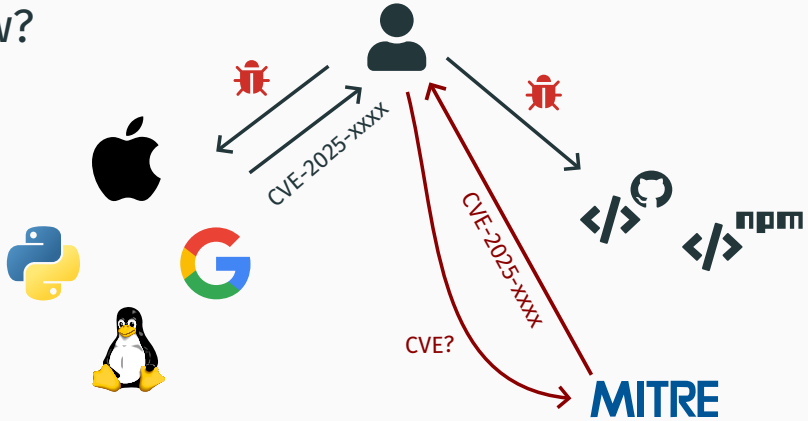
How?



CVE Numbering Authorities (CNAs)

CNAs of **Last Resort** (CNA-LRs)

How?



CVE Numbering Authorities (CNAs)

CNAs of **Last Resort** (CNA-LRs)

=> Lack of Verification!

2 Qualtitative Analysis – By CNA Type

	Agreement	*Don't know*	*No-Info*	*Ignored*	*Opposed*	Sum
CNA-LRs	690	101	158	26	49	1,024
Regular CNAs	499	0	3	0	3	505

2 This has an impact beyond academia

*"But they seem like a known **bad actor**, lots of **bogus CVEs** and no response after that anymore. This is the problem with the whole **security circus**"*

– a project maintainer on GitHub

Let’s compare this data to the opinion of

102 academics

Do you try to obtain CVEs?

Do you try to obtain CVEs? **71%** agree

3 Survey – Authors' Perspective

Do you try to obtain CVEs? **71%** agree

Do CVEs help getting a paper accepted?

3 Survey – Authors' Perspective

Do you try to obtain CVEs? **71%** agree

Do CVEs help getting a paper accepted? **76%** agree

3 Survey – Authors' Perspective

Do you try to obtain CVEs? **71%** agree

Do CVEs help getting a paper accepted? **76%** agree

$\Rightarrow$ CVEs are seen as **desirable**

Do you check submissions for CVEs?

3 Survey – Reviewers' Perspective

Do you check submissions for CVEs? **38%** agree

3 Survey – Reviewers' Perspective

Do you check submissions for CVEs? **38%** agree

Do CVEs improve your perception of a paper?

3 Survey – Reviewers' Perspective

Do you check submissions for CVEs? **38%** agree

Do CVEs improve your perception of a paper? **68%** agree

3 Survey – Reviewers' Perspective

Do you check submissions for CVEs? **38%** agree

Do CVEs improve your perception of a paper? **68%** agree

$\Rightarrow$ **99%** chance that the perception of one of your reviewers is positively affected (assuming four reviewers)

Is verification part of the CVE assignment process?

Is verification part of the CVE assignment process?

54% believe this is the case

Is verification part of the CVE assignment process?

54% believe this is the case

$\Rightarrow$ This may create a false sense of credibility

Takeaways

- **Misaligned incentives** incite a hunt for CVEs
- **Lack of verification** creates opportunity for misuse
- **Misconceptions** lull us into a false sense of security

CVEs are not a good impact metric