

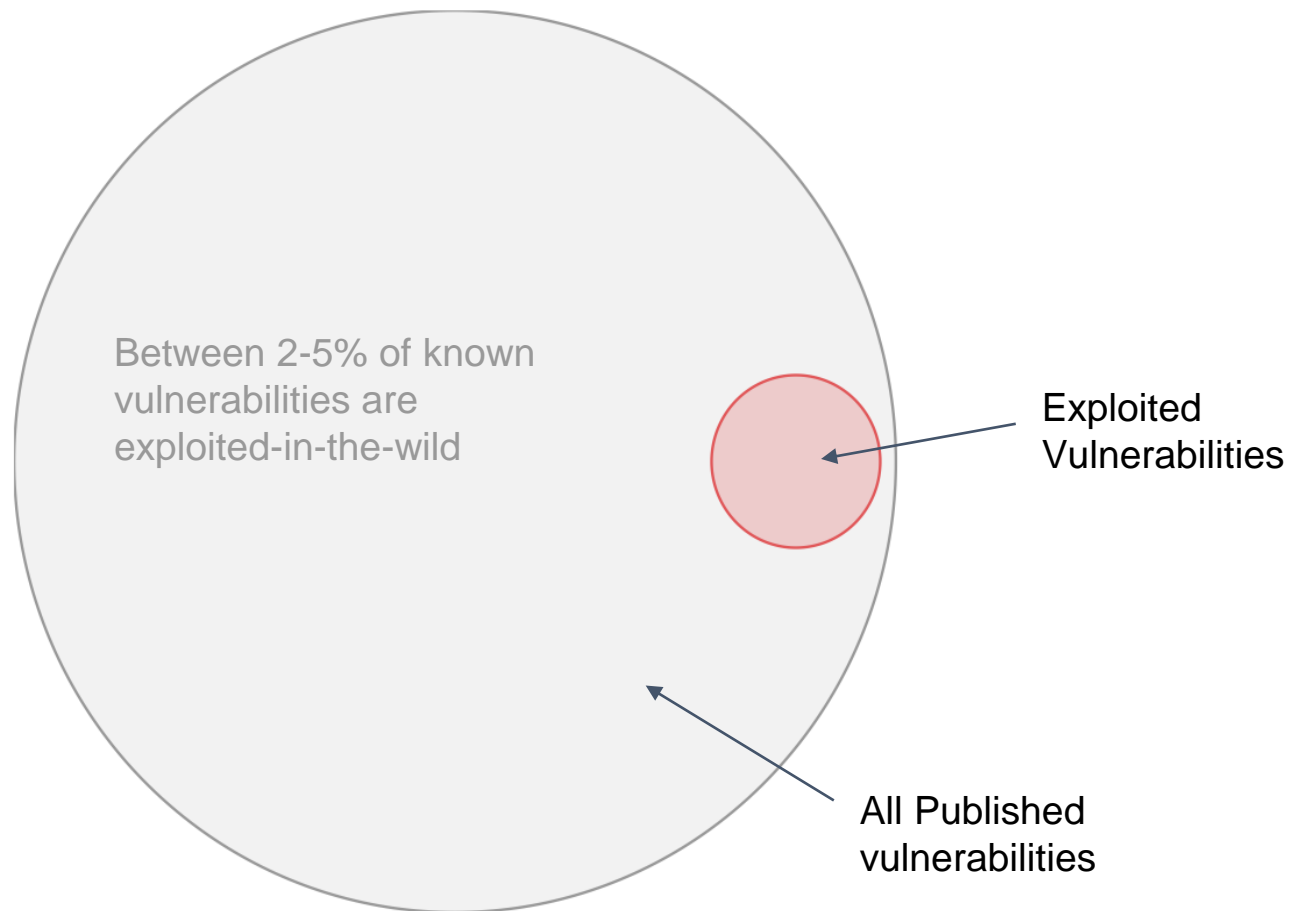


Exploit Prediction Scoring System (EPSS)

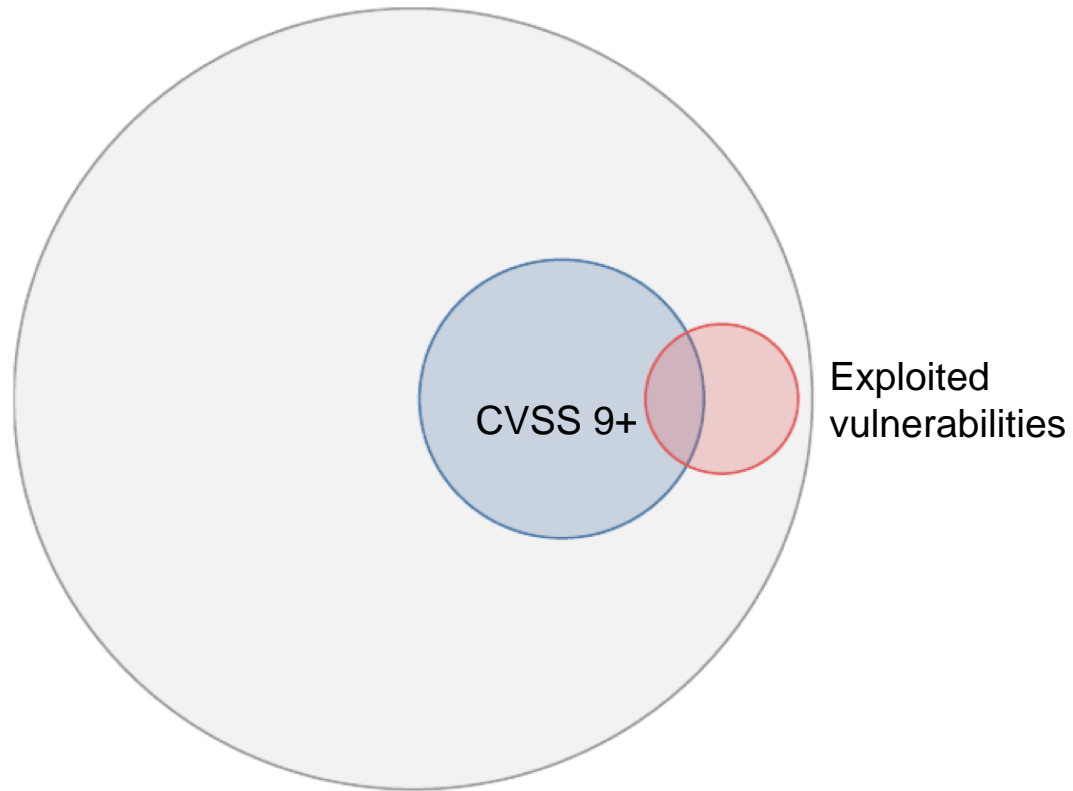
Changing our approach to vulnerability prioritization

Sasha Romanosky
December 7, 2022

The Problem



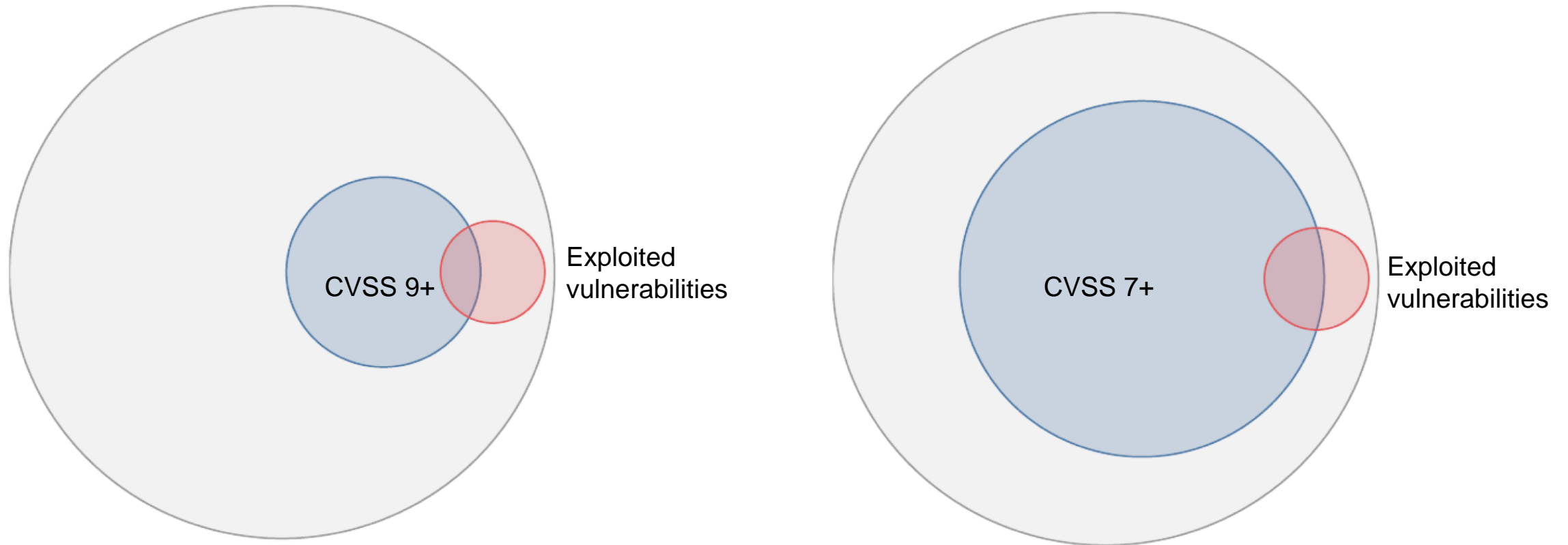
Current prioritization strategies are highly inefficient



A) Patch strategy of CVSS 9+

Common Vulnerability Scoring System (CVSS), the de facto way of prioritizing vulnerabilities

Current prioritization strategies are highly inefficient



A) Patch strategy of CVSS 9+

B) Patch strategy of CVSS 7+

Common Vulnerability Scoring System (CVSS), the de facto way of prioritizing vulnerabilities

We need a better solution



- We lack an **objective** way of understanding the actual threat of vulnerabilities – that is, a way to estimate which vulnerabilities will be exploited
- The data have existed, but no one has thought to use them

What is EPSS?

- The Exploit Prediction Scoring System (EPSS) is an open, data-driven framework for estimating the probability that a vulnerability will be exploited
 - Leverages evidence of **actual exploitation**
 - Produces scores between 0-1 (or 0-100%)
 - Scores are **freely** available for all 180,000+ vulns
 - See https://www.first.org/epss/data_stats

Download the data

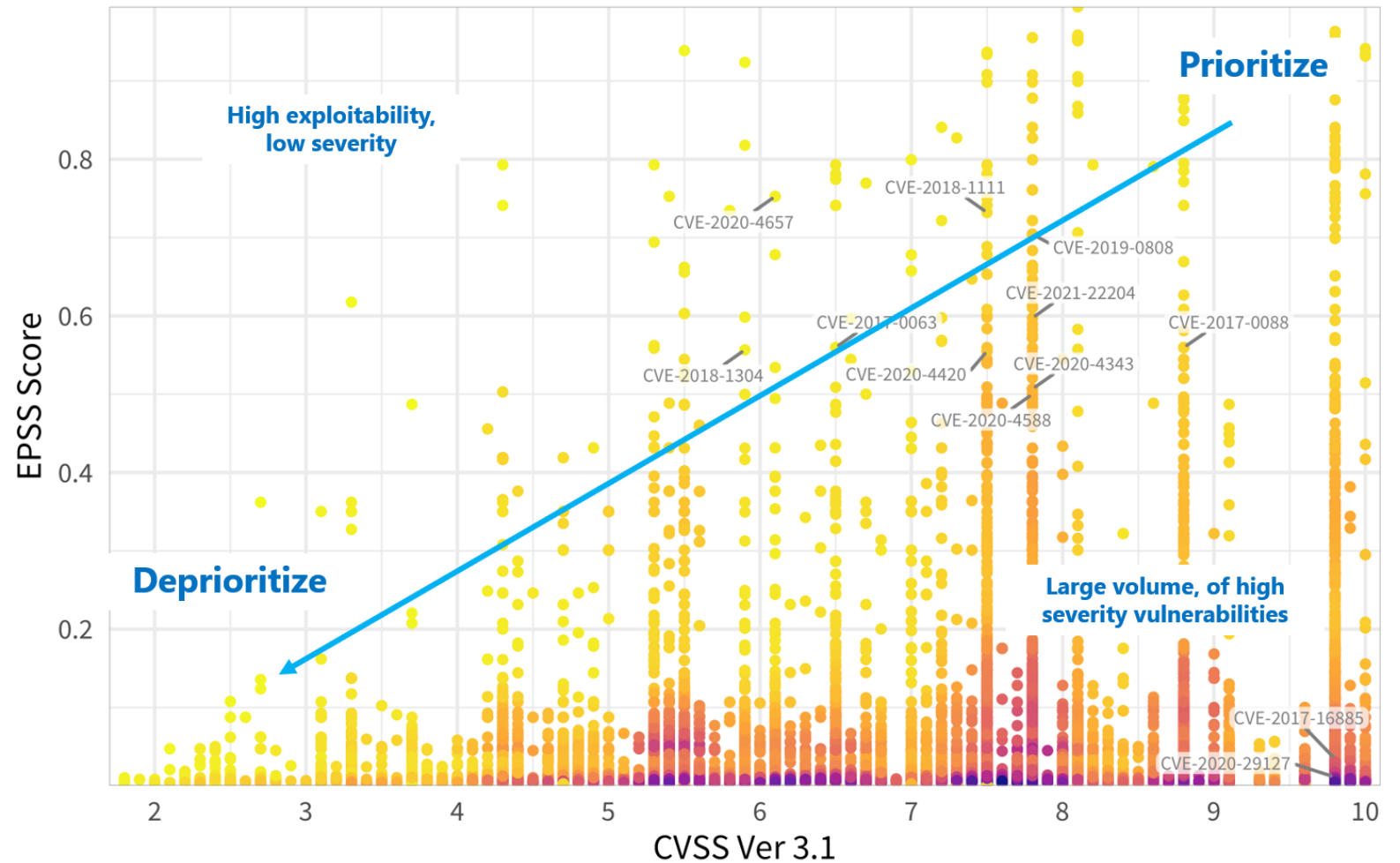
What is EPSS?



- EPSS is a special interest group (SIG) organized under the Forum of Incident Response and Security Teams (FIRST)
 - See <http://www.first.org/epss>
 - Composed of 150+ researchers, academics, practitioners, and Govt and UK representatives
 - SIG and Slack are open to anyone looking to join and participate
- Published Papers
 - Jay Jacobs, Sasha Romanosky, Benjamin Edwards, Michael Roytman, Idris Adjerid, (2021), *Exploit Prediction Scoring System*, ACM Digital Threats Research and Practice, 2(3).
 - Jay Jacobs, Sasha Romanosky, Idris Adjerid, Wade Baker, (2020), *Improving Vulnerability Remediation Through Better Exploit Prediction*, Journal of Cybersecurity, 6(1), <https://doi.org/10.1093/cybsec/tyaa015>.

What can we do with EPSS?

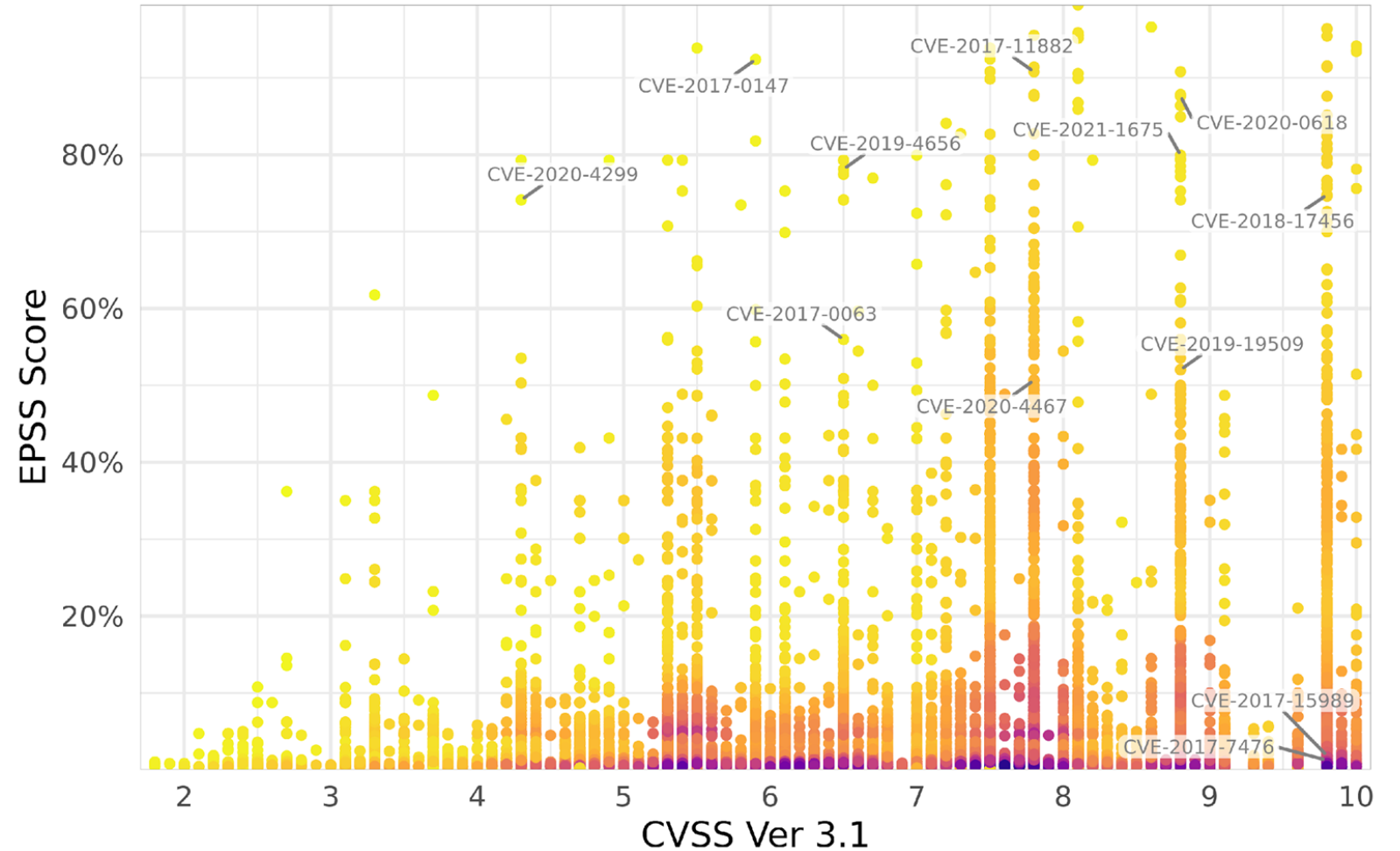
#1: Plot your organization's attack surface



Source: https://first.org/epss/data_stats, 2021-05-16

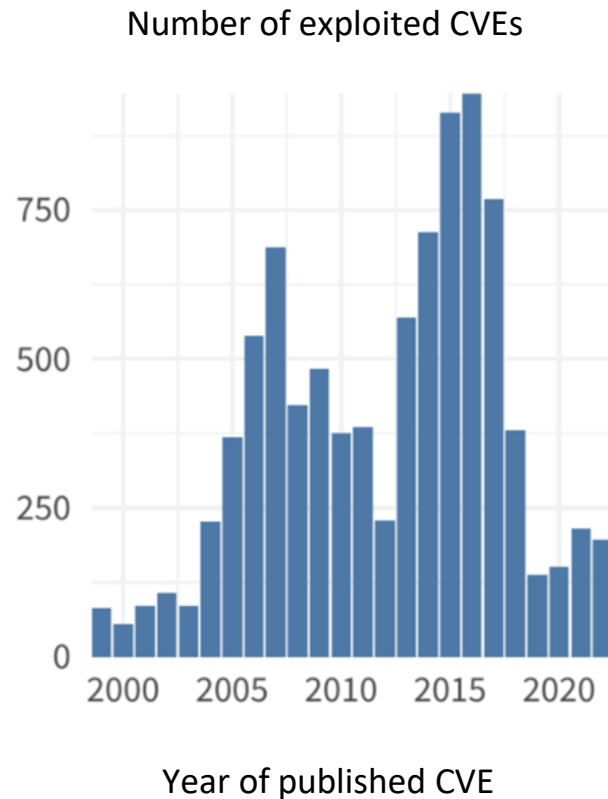
What can we do with EPSS?

#2: View your organization's SBOM



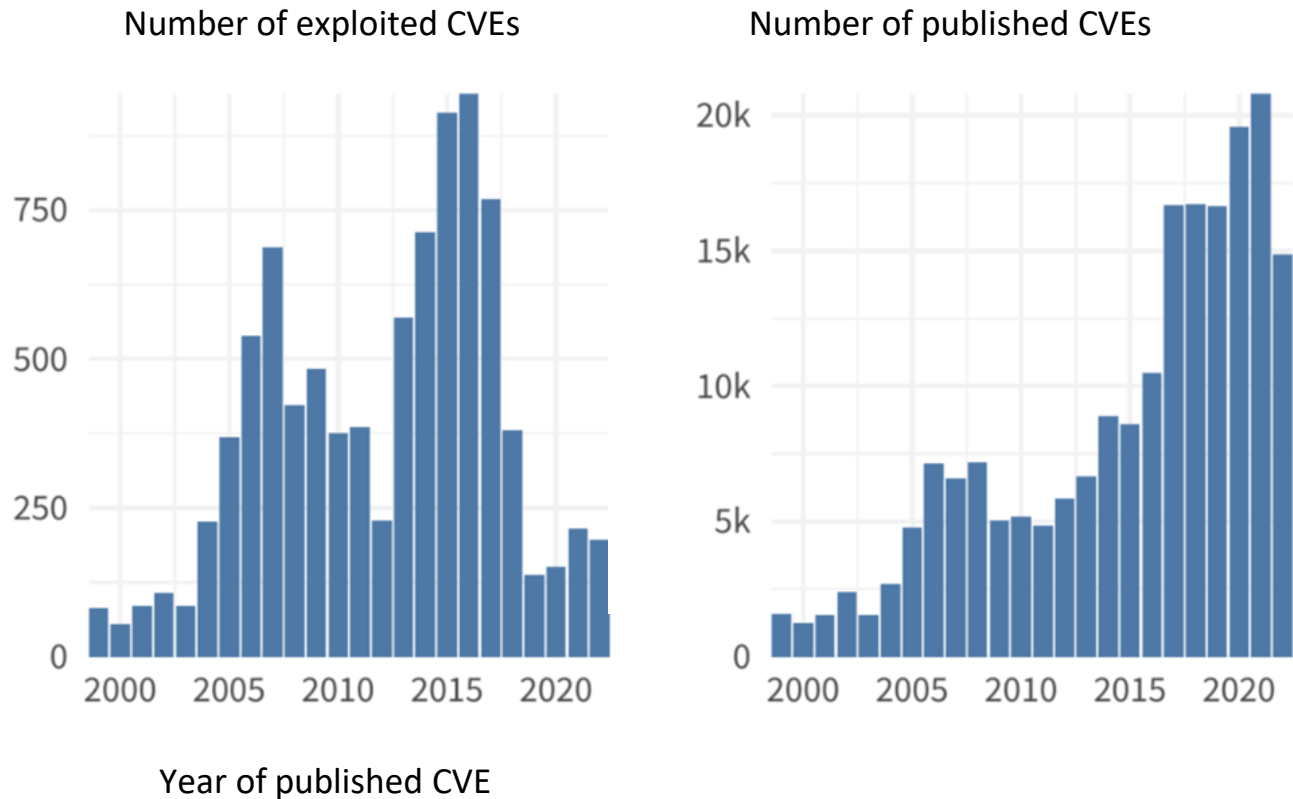
Source: https://first.org/epss/data_stats, 2021-10-27

How many vulnerabilities are being exploited, anyhow?



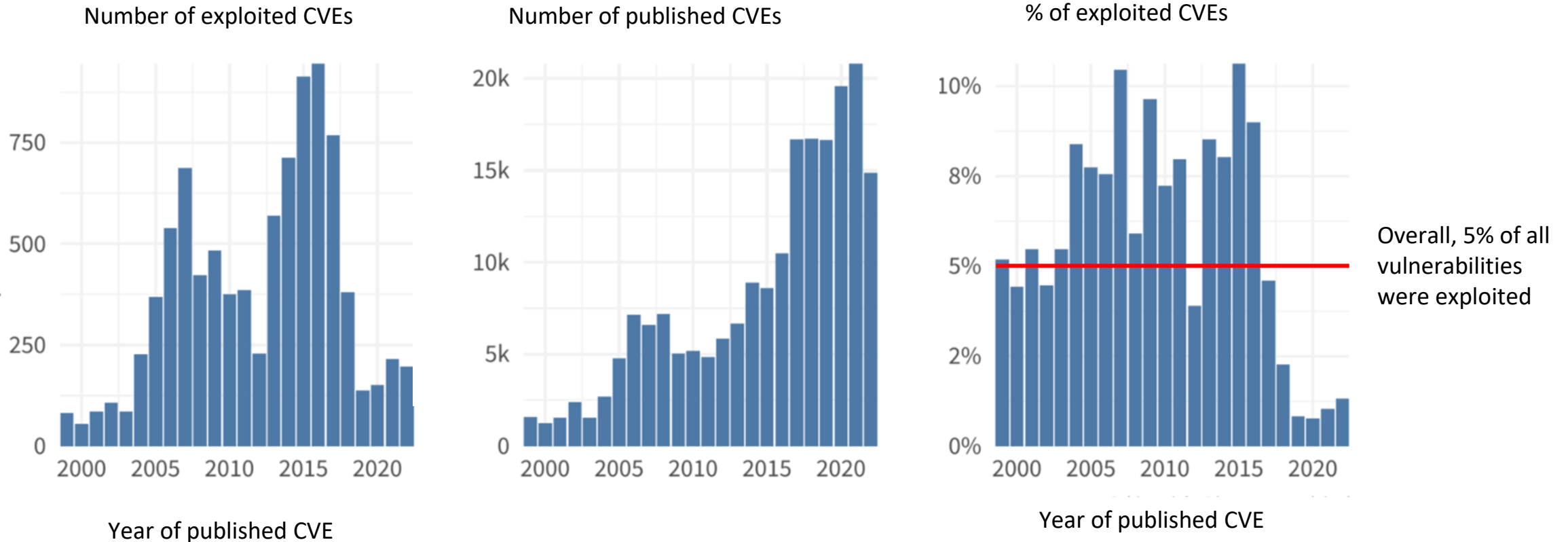
- Over an 8 year period, we observed 5.2 million exploit attempts
- Targeting over 9000 unique vulnerabilities

How many vulnerabilities are being exploited, anyhow?



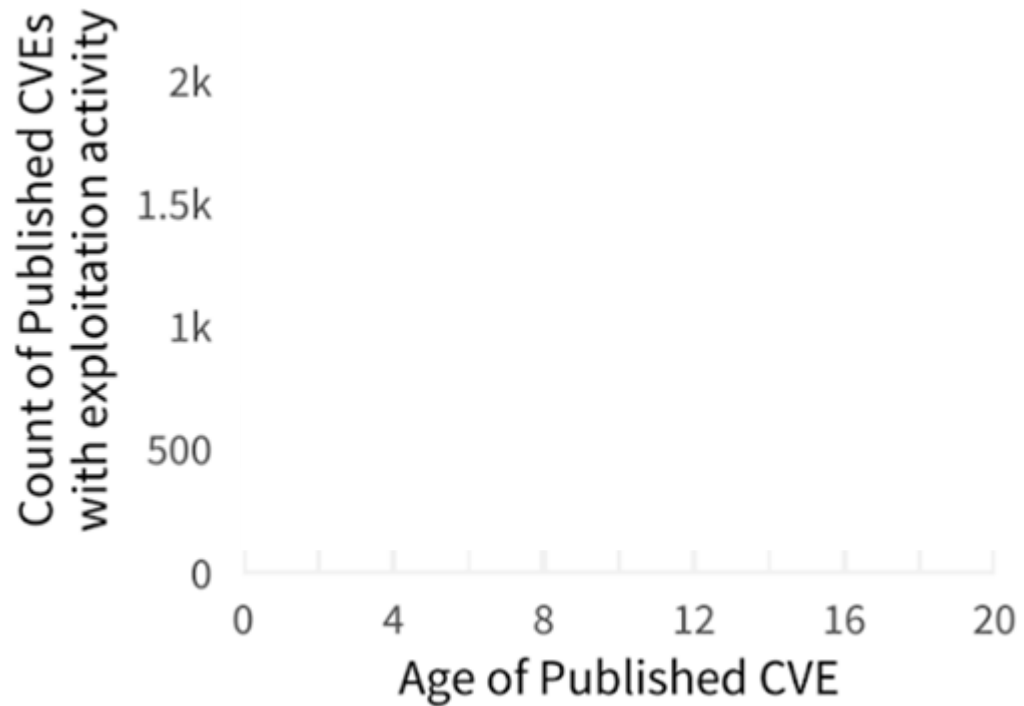
- The rate of vulnerability disclosures has been increasing dramatically since 2000

How many vulnerabilities are being exploited, anyhow?



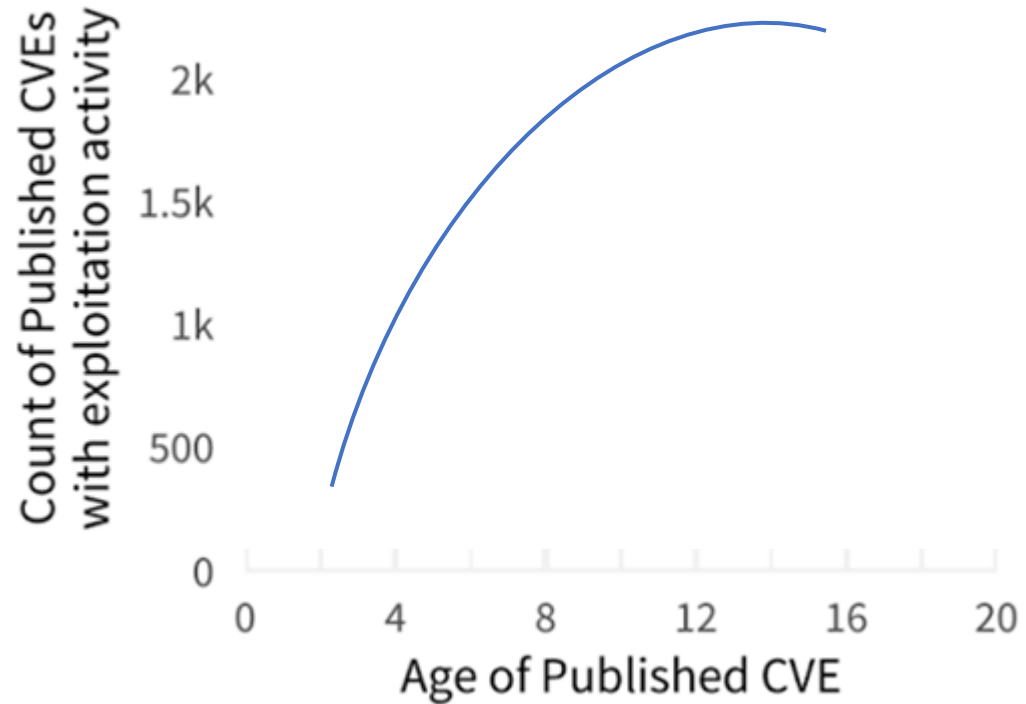
- Further evidence that despite rampant attention about data breaches and cyber incidents, very few vulnerabilities are ever exploited

Are vulnerabilities exploited more or less over time?



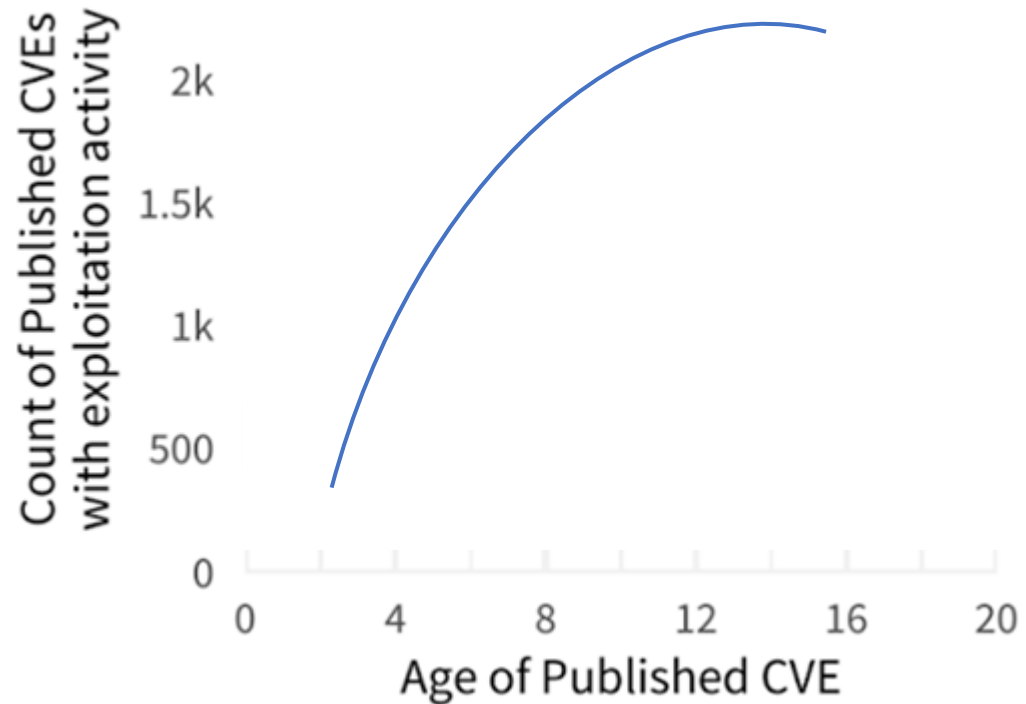
Are vulnerabilities exploited more or less over time?

They might be exploited **more** over time, as more info is collected, better, easier exploit code becomes available

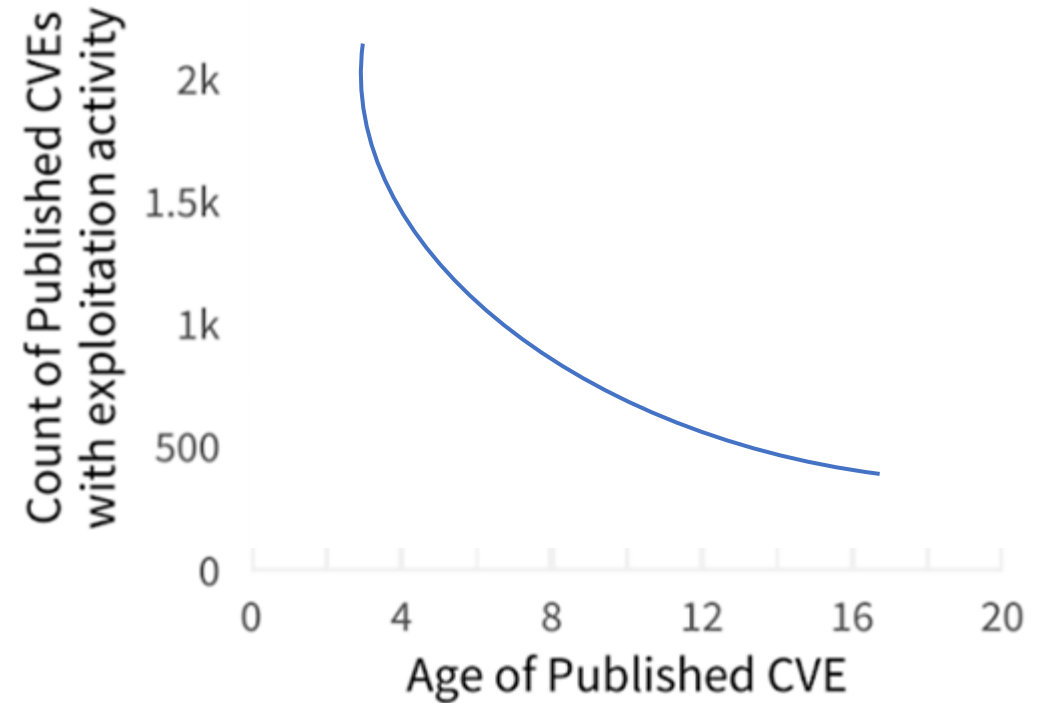


Are vulnerabilities exploited more or less over time?

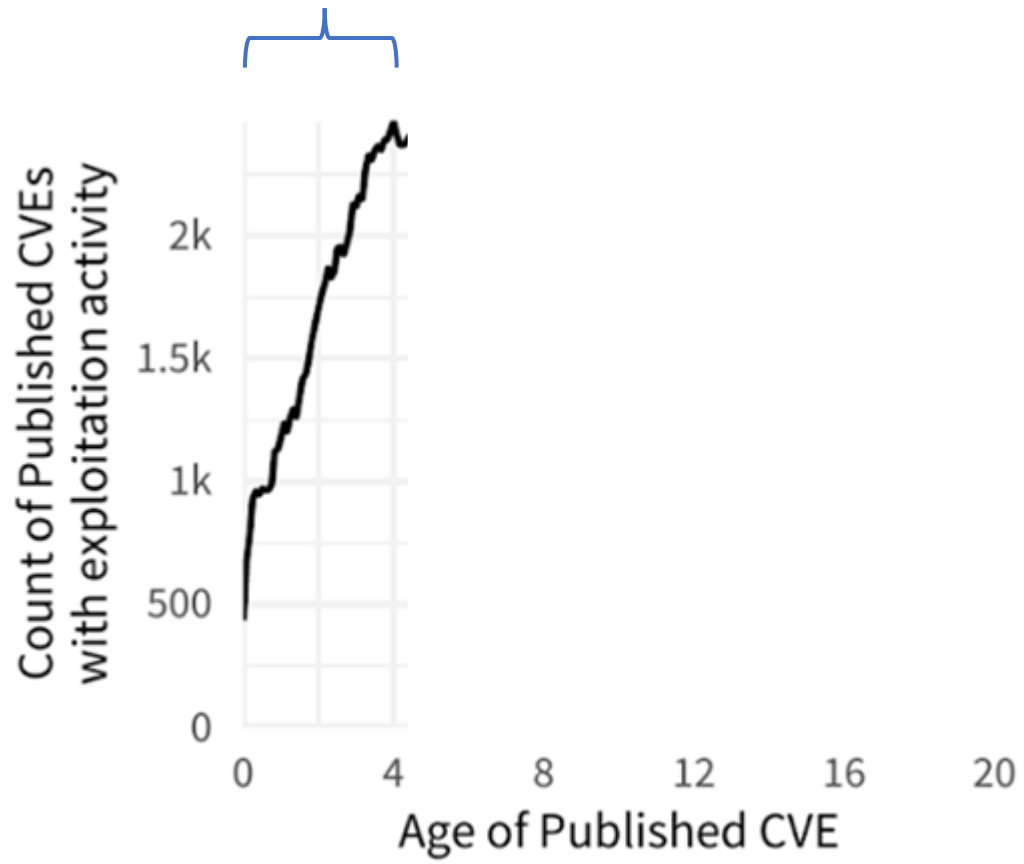
They might be exploited **more** over time, as more info is collected, better, easier exploit code becomes available



They might be exploited **less** over time, as firms patch, and hackers discover new vuln

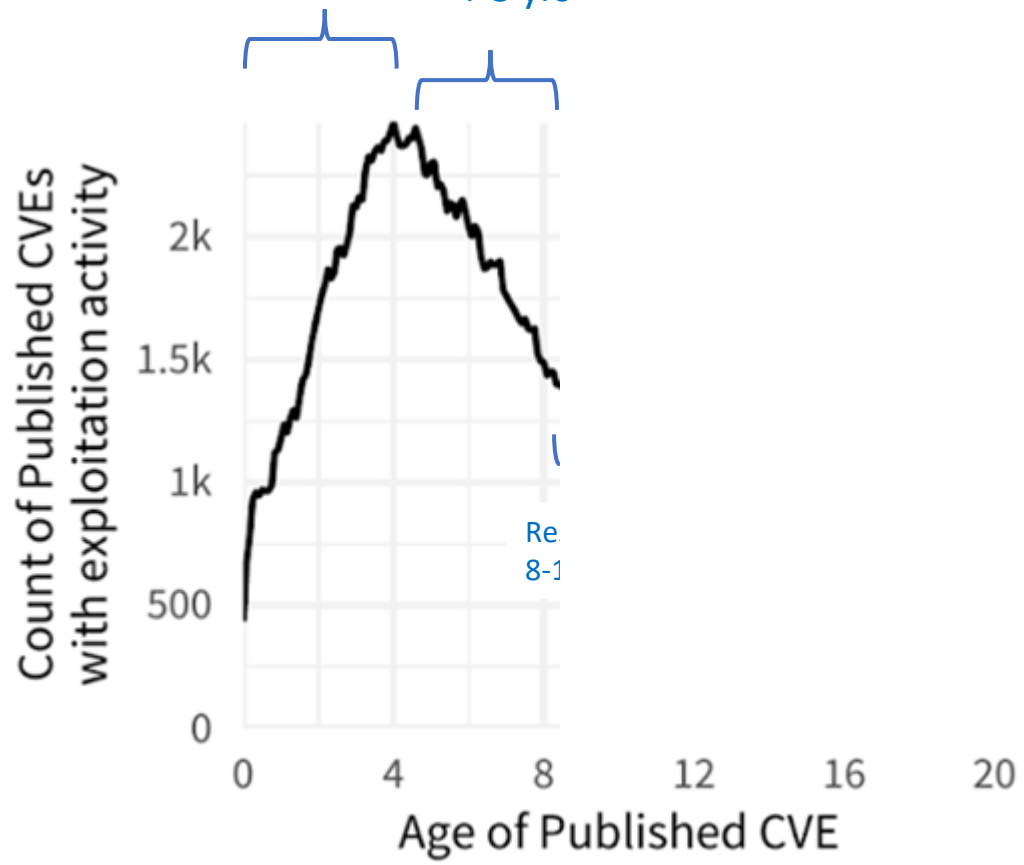


Vulnerabilities are exploited more and more, until 4 yrs old



Vulnerabilities are exploited more and more, until 4 yrs old

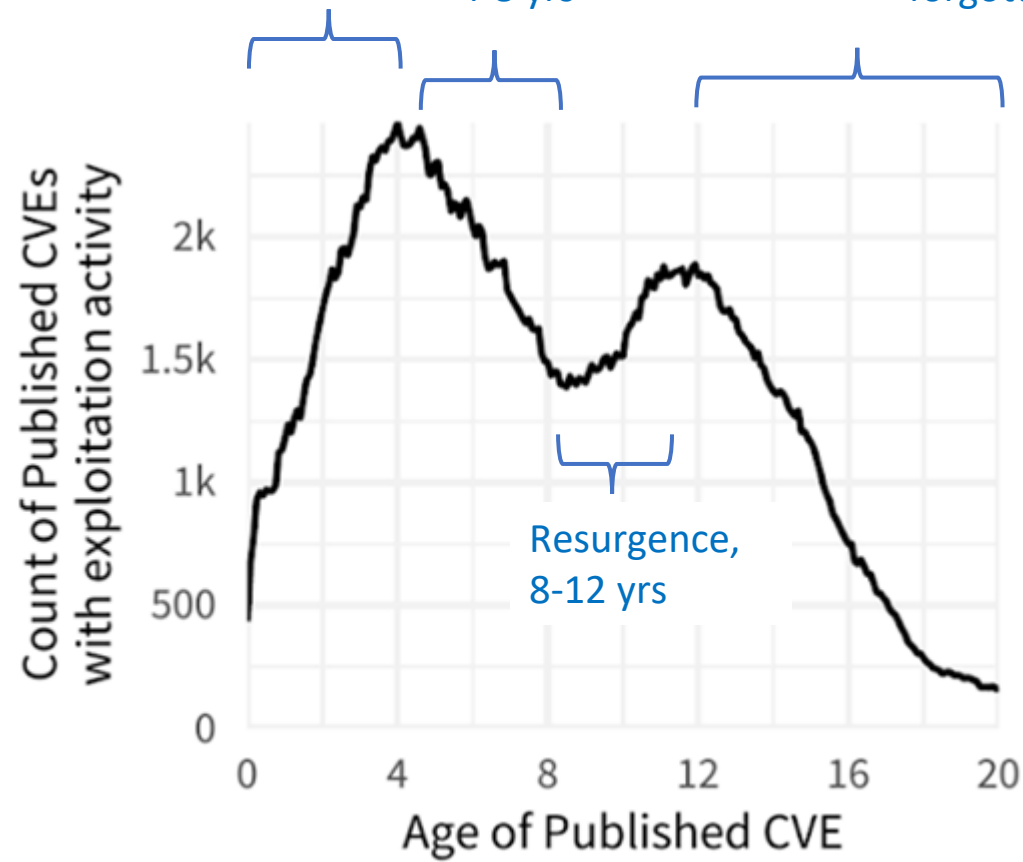
Declining interest, 4-8 yrs



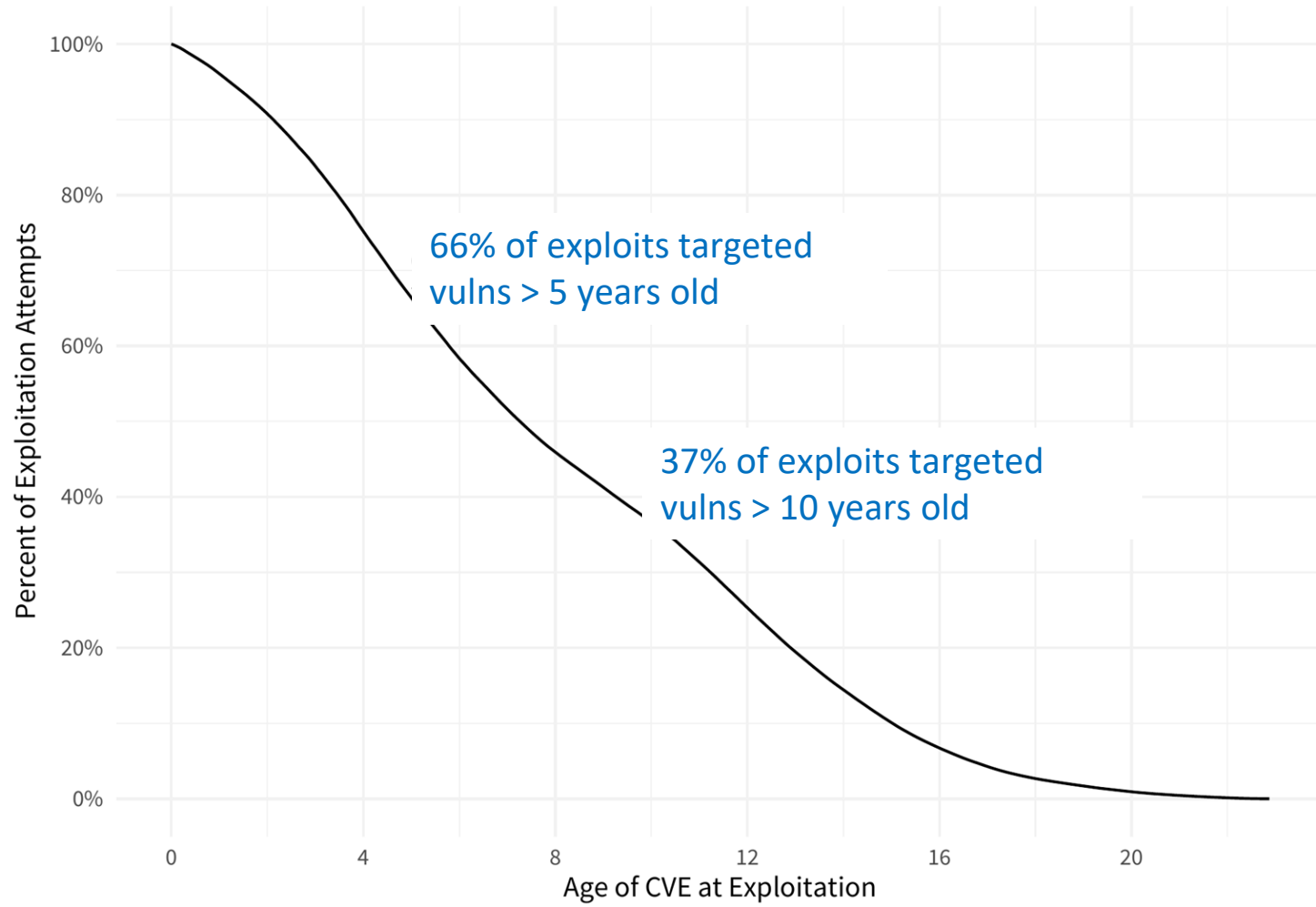
Vulnerabilities are exploited more and more, until 4 yrs old

Declining interest, 4-8 yrs

Older, but not forgotten, 12-20 yrs

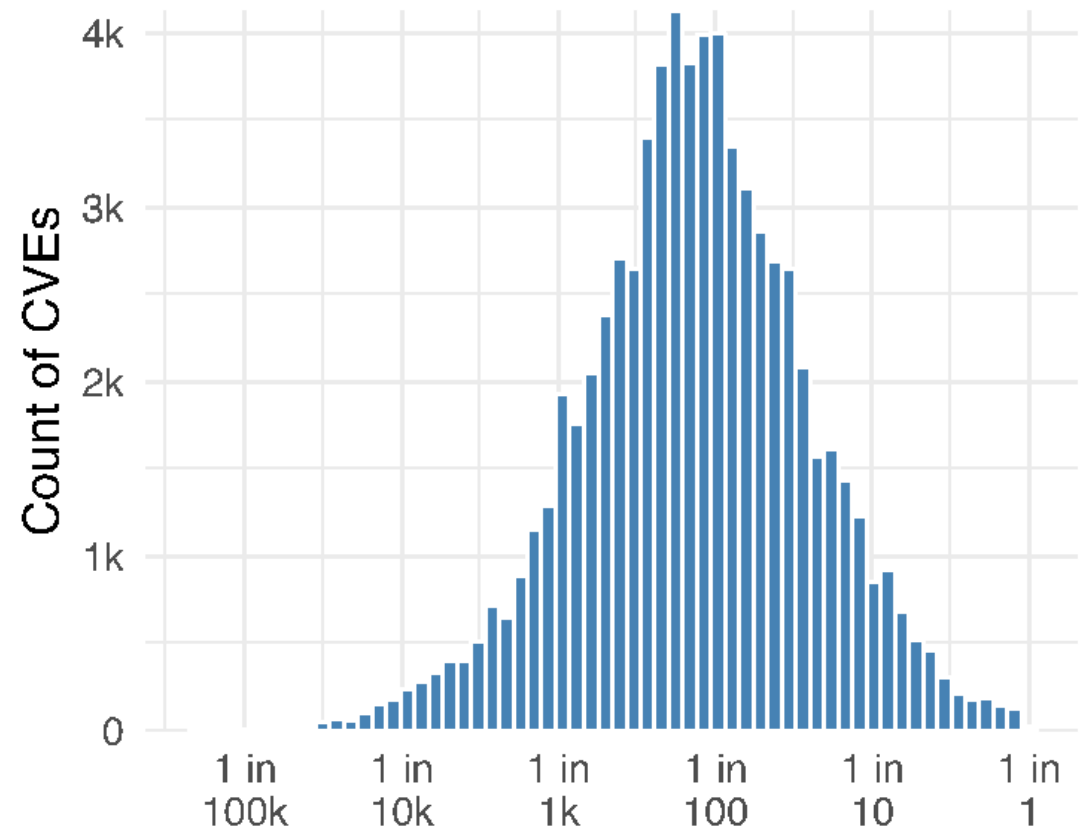
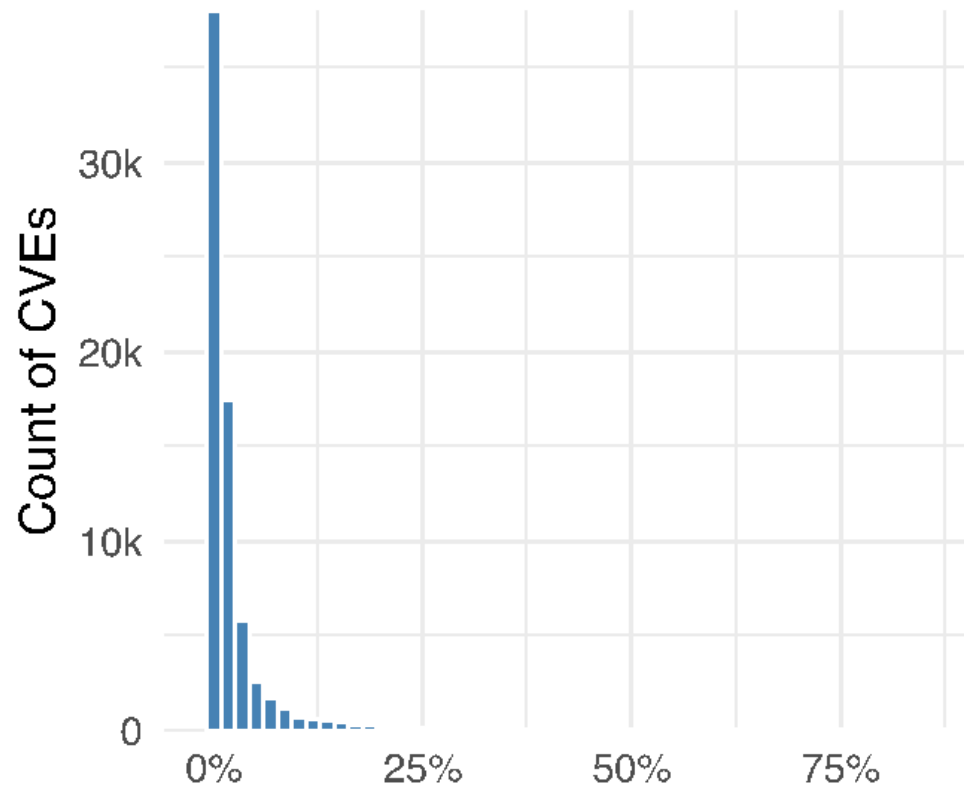


Are hackers exploiting newer or older vulnerabilities?



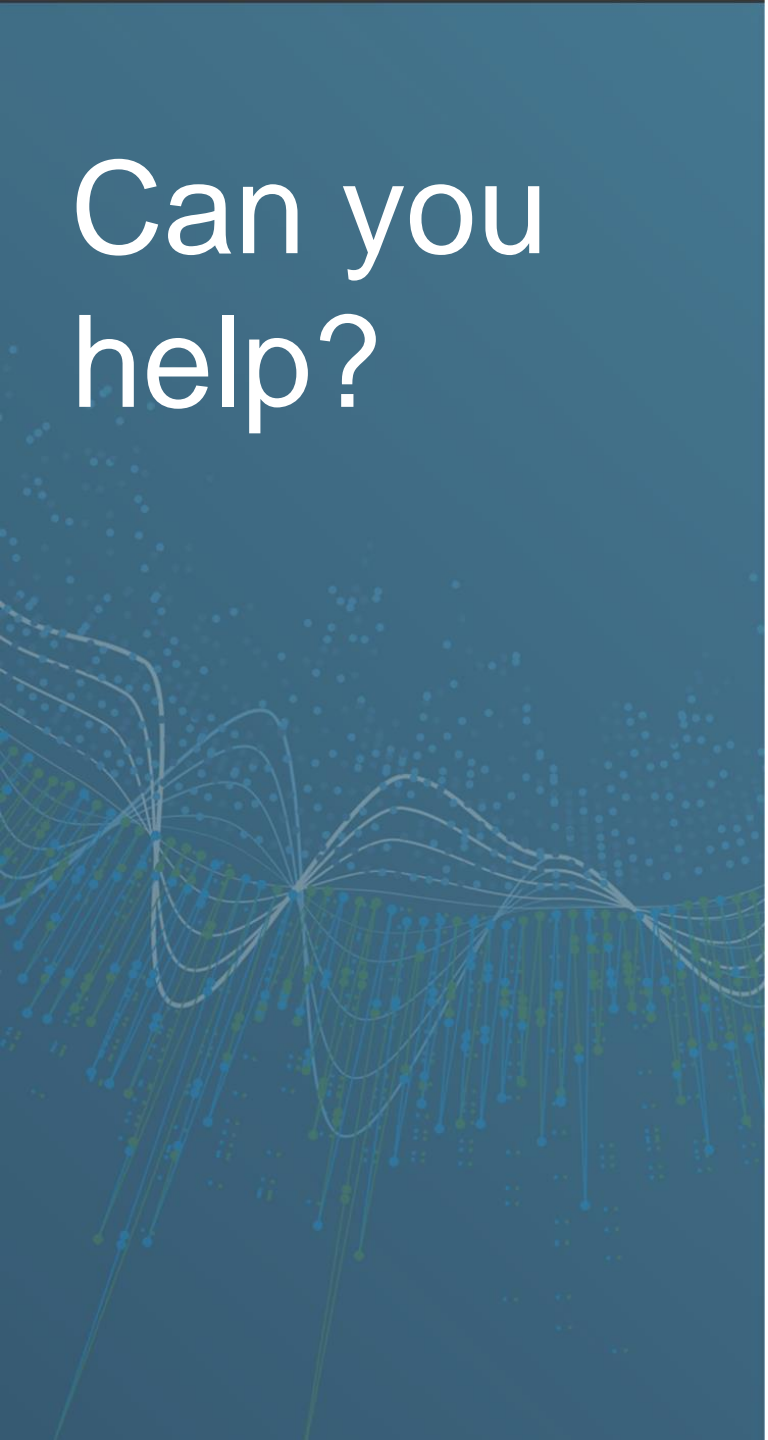
This is crazy

How to best convey probabilities?



Probability of exploitation

Can you help?



YES! In two ways:

- 1. Try it out!** Download the data (https://www.first.org/epss/data_stats) and tell us if they make sense, and help you better prioritize
- 1. Help us find new sources of exploit data!**
We are always looking for more organizations to partner with. Data could come from IDS/IPS, network observatories, honeypots, other network sensors

Contact epss-chairs@first.org with any questions



Questions?

@SashaRomanosky@techhub.social

sromanos@rand.org

