Updates from the CVSS SIG

CVSS v4.0 By the Numbers

Nick Leali

April 8, 2025

Updates from the CVSS SIG Overview

- A Year of CVSS v4.0
- CVSS SIG Work to Date
- CVSS v4.0 survey
- Near future work of CVSS SIG

Whoami

- Nick Leali
- Cisco PSIRT
- CVSS SIG co-chair
- User of CVSS since 2009
- Very, very amateur software developer

Pictured: A natural reaction to CVSS

Thank You to the CVSS SIG

CVSS

COMMON VULNERABILITY SCORING SYSTEM

A Year of CVSS v4.0

- CVE Program and NVD support CVSS v4.0 vectors
- CVE Program: 4814 CVSS v4.0 vectors
- GitHub: 7229 CVSS v4.0 vectors (3334 reviewed, 3895 unreviewed)
- Vendor support: 56 unique vendors in the CVE Program
- More about the numbers later!

CVSS SIG Work to Date

Document updates

Examples

FAQ

Tooling support

CVE Program and NVD

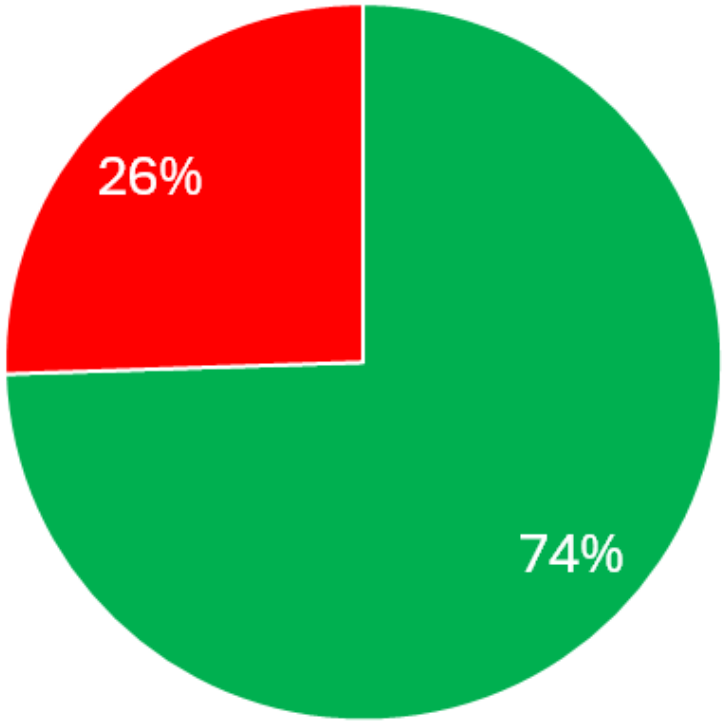
Red Hat library

Many third-party tools

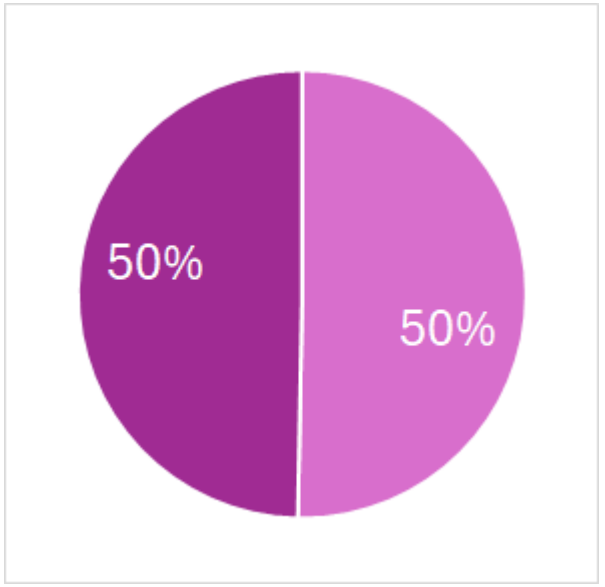
Resources testing

Results of the CVSS Survey

Opinions on CVSS v4.0

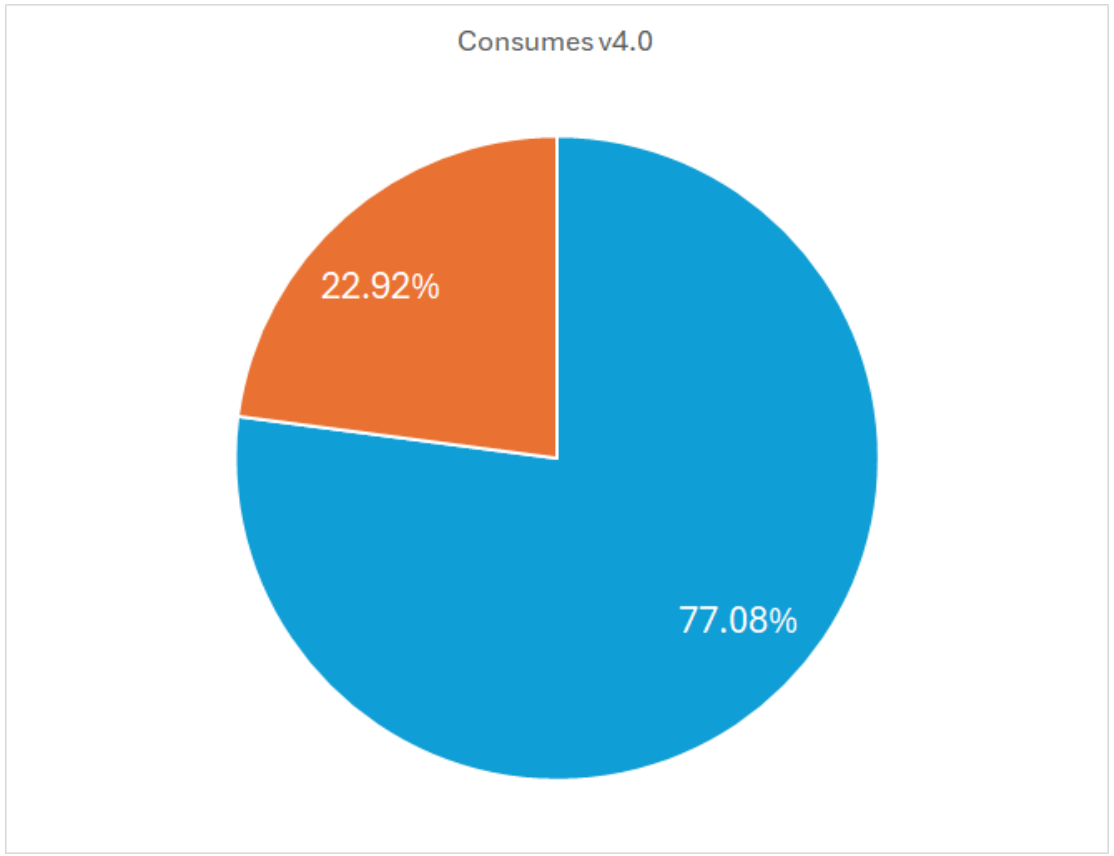


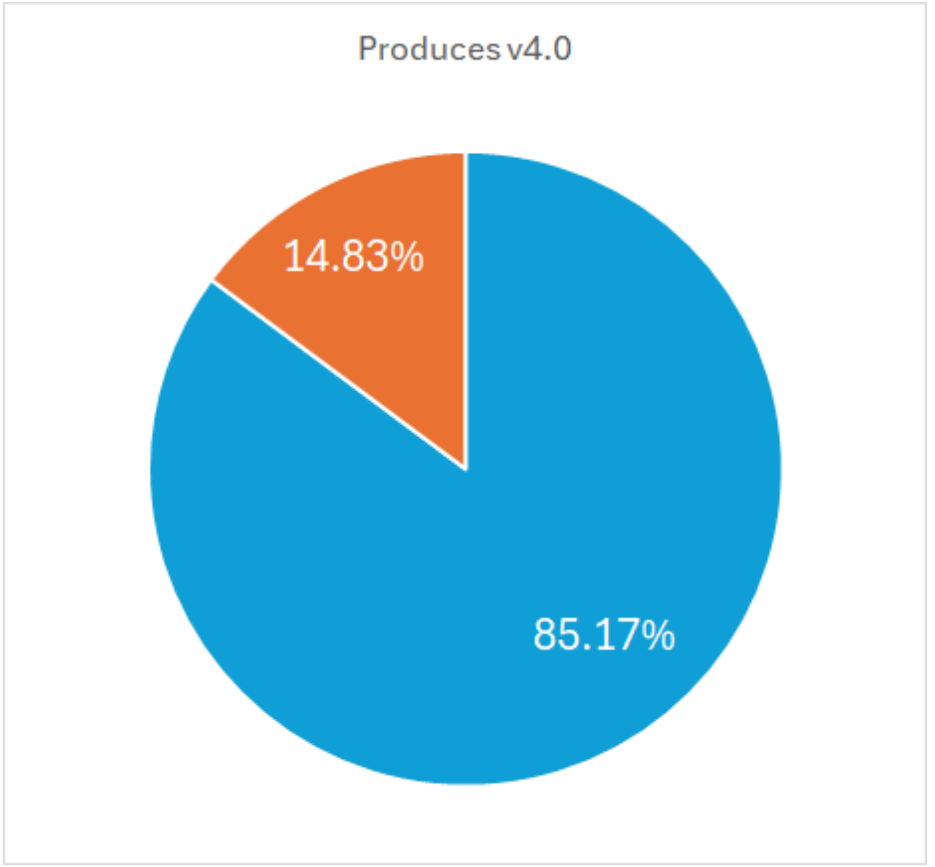
All survey respondents



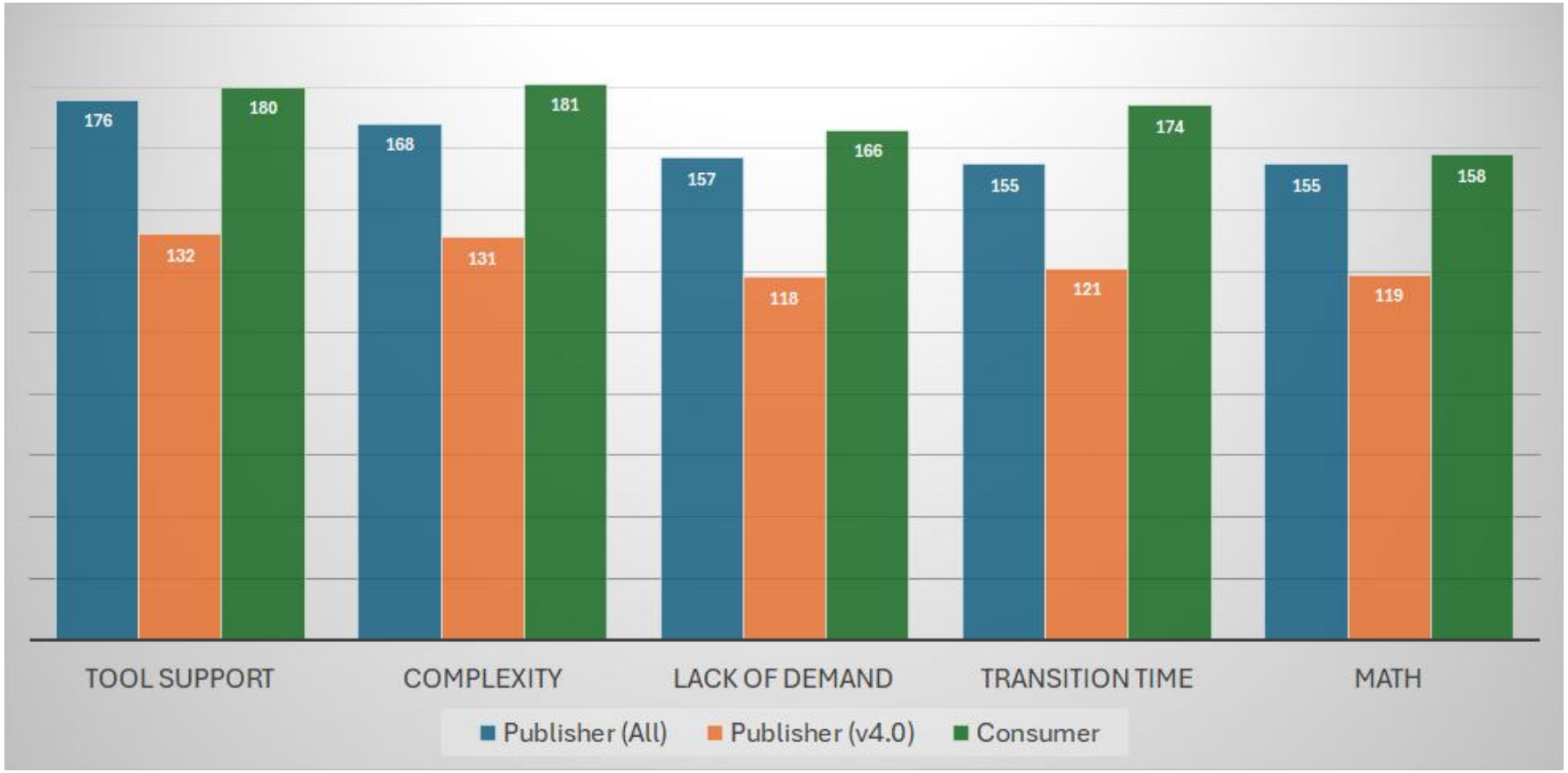
No usage of CVSS v4.0

CVSS v4.0 Opinion Among Adopters

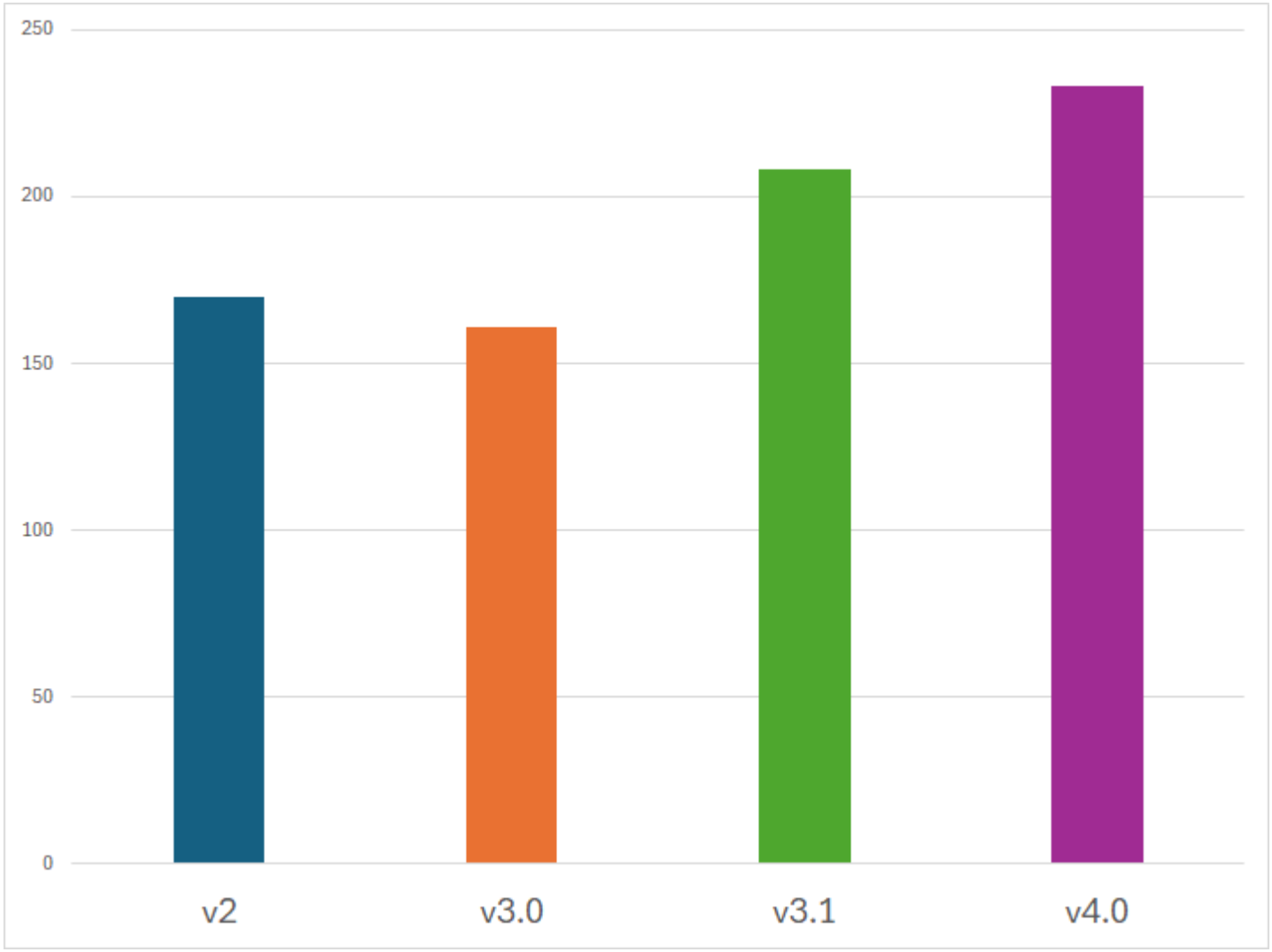




Challenges to v4.0 Adoption



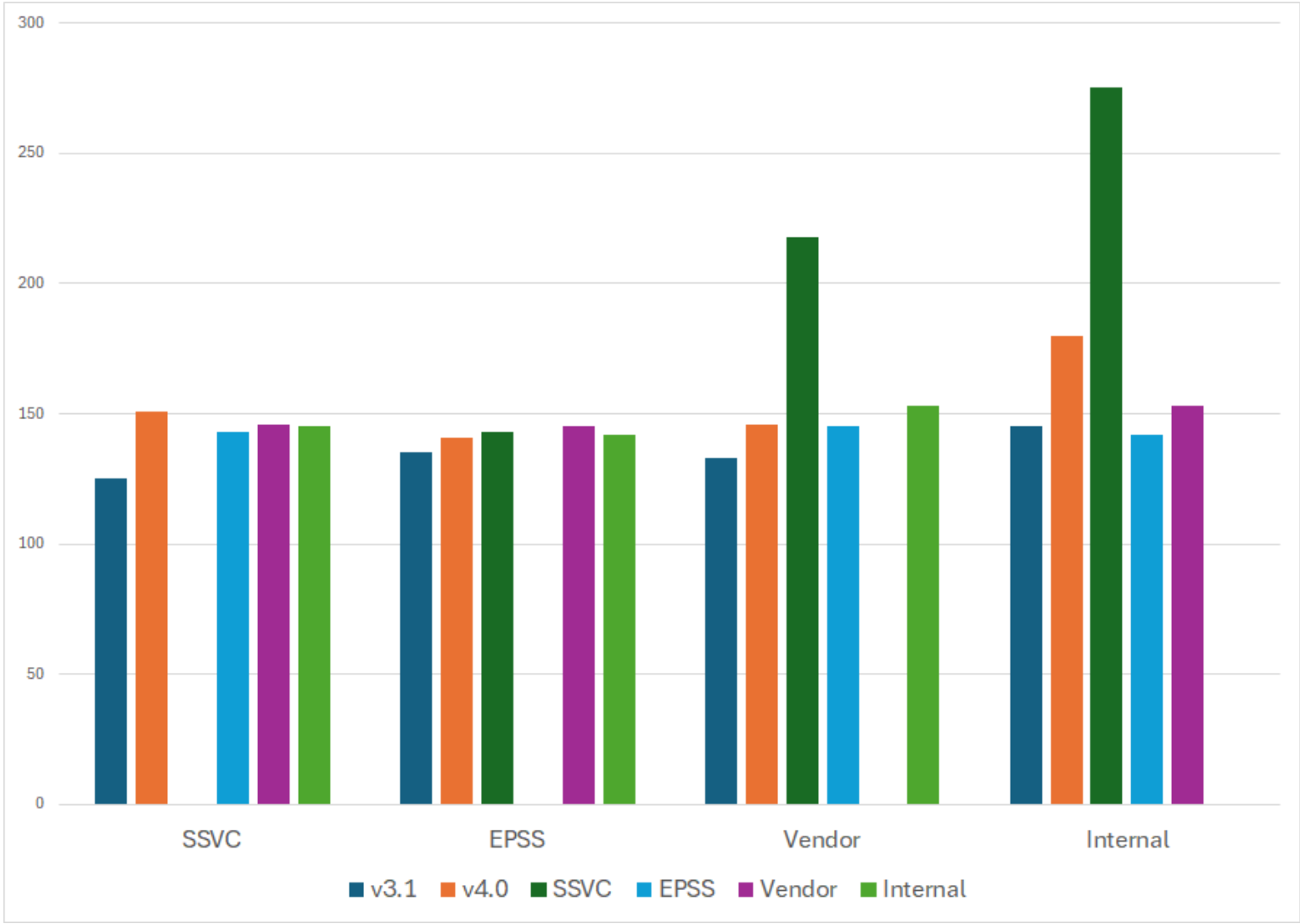
CVSS Usage Among Respondents



- Usage among producers
- All versions of CVSS represented
- Very long tail on CVSS v2.0

Consumers Combine Other Systems With CVSS

- CVSS not used alone
- Many other systems are used, and in combination
- 37% of respondents use 2 or more systems



Where the SIG is Heading

Enhanced User Guide	• Providing implementation advice for end consumers
More Examples and documentation	• CVSS vector enrichment
Per-product Assessments	• Impacts of CVEs per platform
Gathering revisions for future 4.1	• Not in 2025!

Get Involved

CVSS is the most convoluted vulnerability assessment standard

Come help us make it even more complicated!

Feedback or discussion welcome

Examples and more

Up next:

CVSS v4.0 By the Numbers!

Questions?

Thanks!

FIRST™
Improving Security Together

CVSS v4.0 By the Numbers

Nick Leali

April 8, 2025

CVSS v4.0 By the Numbers Overview

- CVSS v4.0 is Different
- Review v3.1 and v4.0 Data
- Lessons from the Data
- Questions and Resources

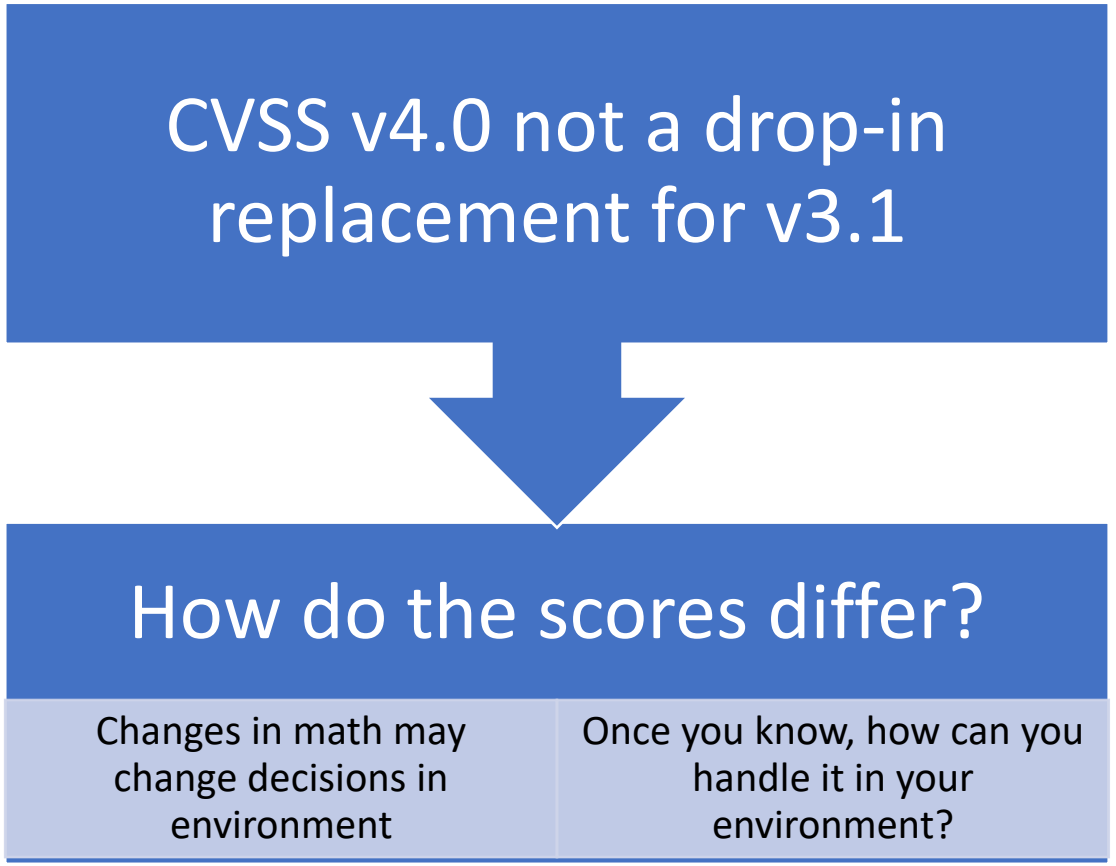
CVSS v4.0 Is Different

How can you prepare to adopt the new standard.

This Is New Math

Who is this for?

- Incident handlers
- Vendors who are considering CVSS v4.0 support
- CVSS consumers who want to start handling CVSS v4.0 vectors



Why care about the numbers?

- Customers ask about it all the time
- Vulnerability disclosure decisions

Our security vulnerability, and others
Is this a blind spot?

- Incident response SLA

The specter of CRA and the like

- Contractual obligations
- Compliance

Baked into PCI-DSS

Comparing v3.1 to v4.0

Math lessons.

Sources of CVSS Data

- Public Cisco CVEs
- CVE program JSON
- GitHub advisories, reviewed and unreviewed
- NVD
- CISA KEV
- ALL THE SCORES

Compare v3.1 scores to v4.0

Checks sources of data for pairs of CVSS vectors

CSV or JSON

Checks the pairs for various statistics with numpy

Will describe those stats shortly!

Graphs those with matplotlib

Scores and score differences

Todo

More data sources (CISA KEV, All CVSS vectors)

CVSS Data Terminology

Record count

Average change

- Average between each v3.1 and v4.0 pair

Mode

- Most common change
- Caution: strange results

Qualitative boundary shift

- Ratio of changes
- Types of changes

Range

- Overall change between biggest and smallest change

Qualitative Boundaries

Low: Up to 3.9

Medium: Between 4.0 and 6.9

High: Between 7.0 and 8.9

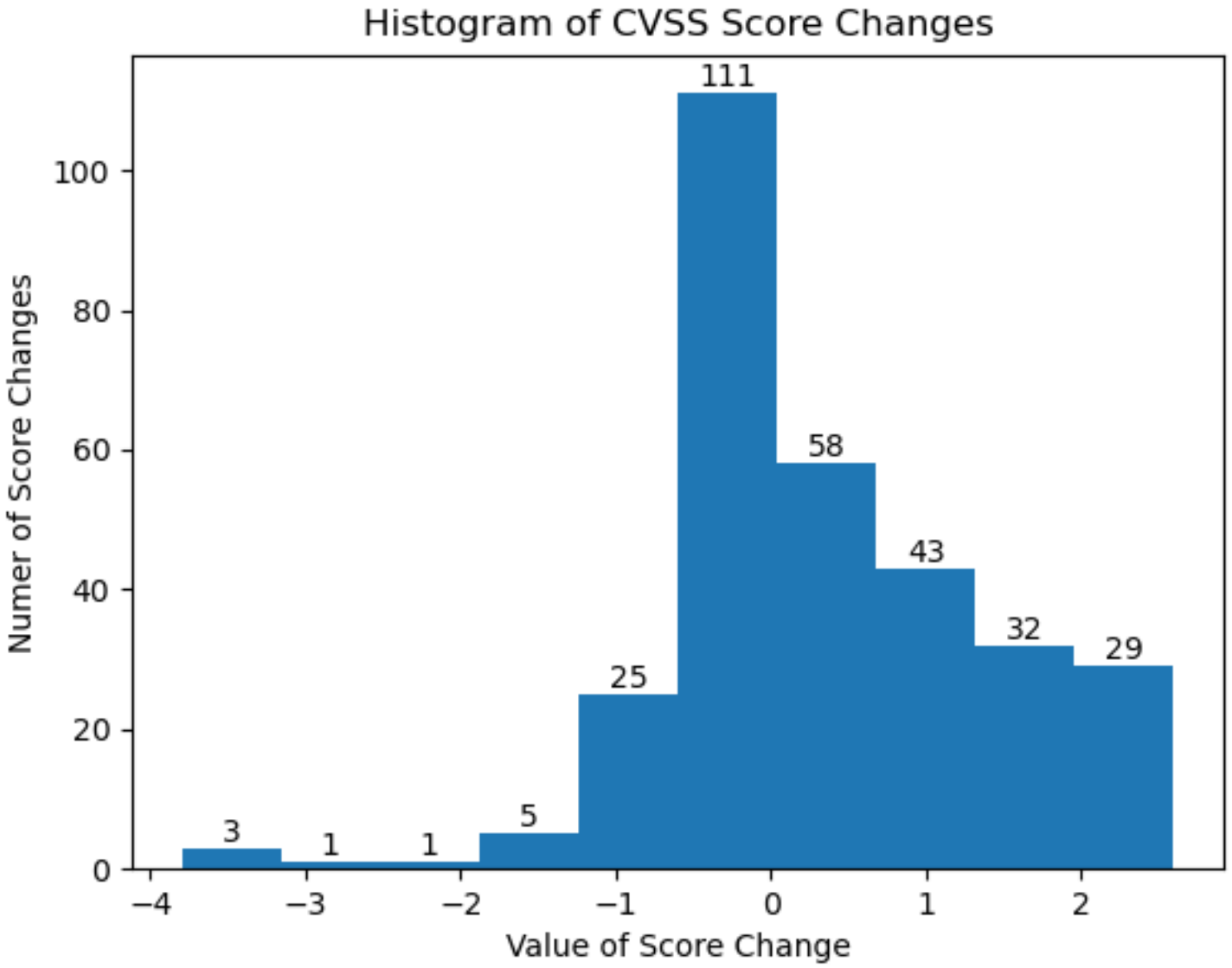
Critical: 9.0 and above

Data Overview

Comparing CVSS v3.1 to CVSS v4.0

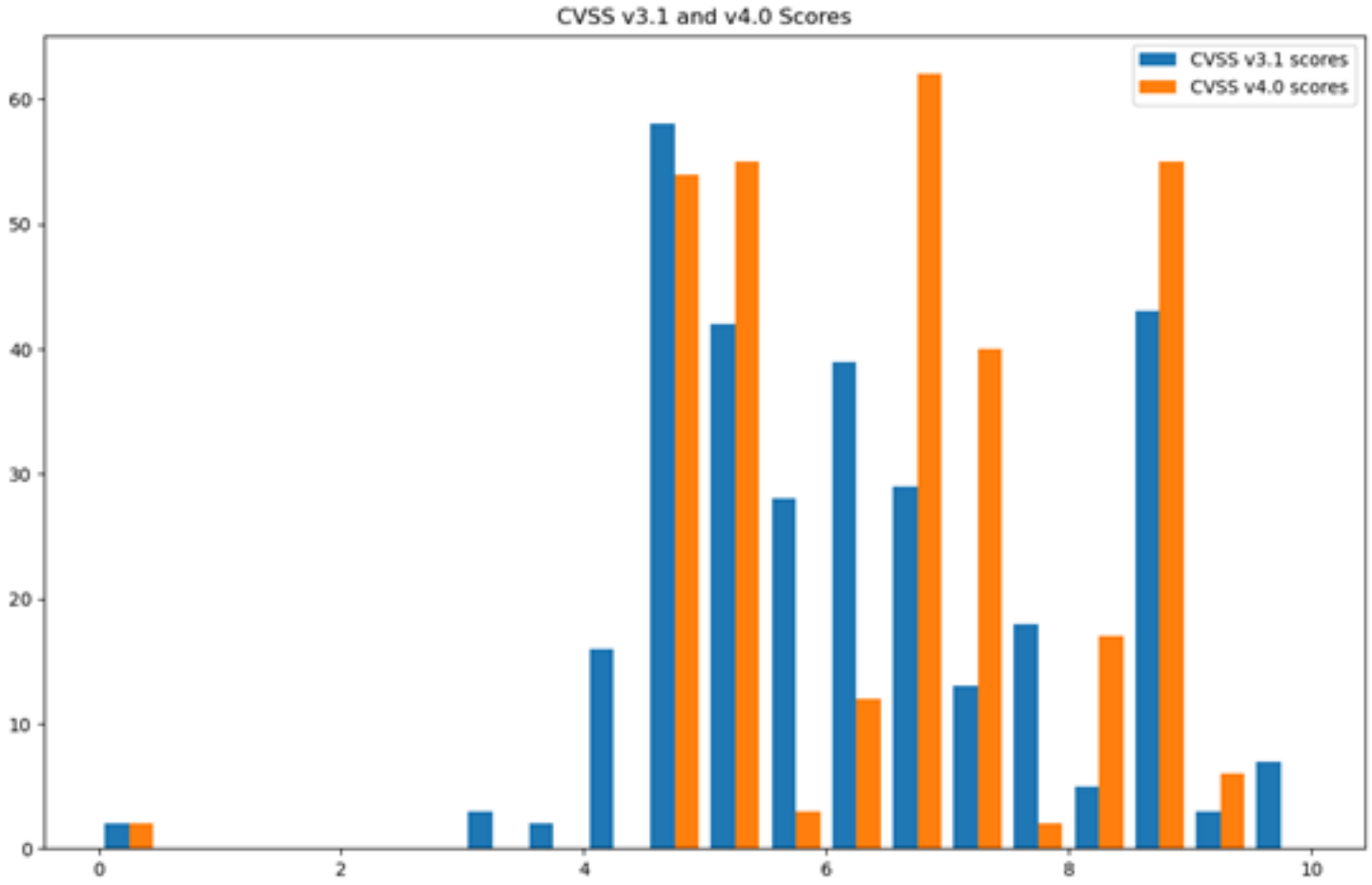
Cisco Study – Public CVEs

- 308 records
- Average change
  - 0.36
- Mode
  - 0.0
- Qualitative boundary shift
  - 15% (49 out of 308)
- Range
  - Increase: 2.6
  - Decrease: -3.8
  - Total: 6.4



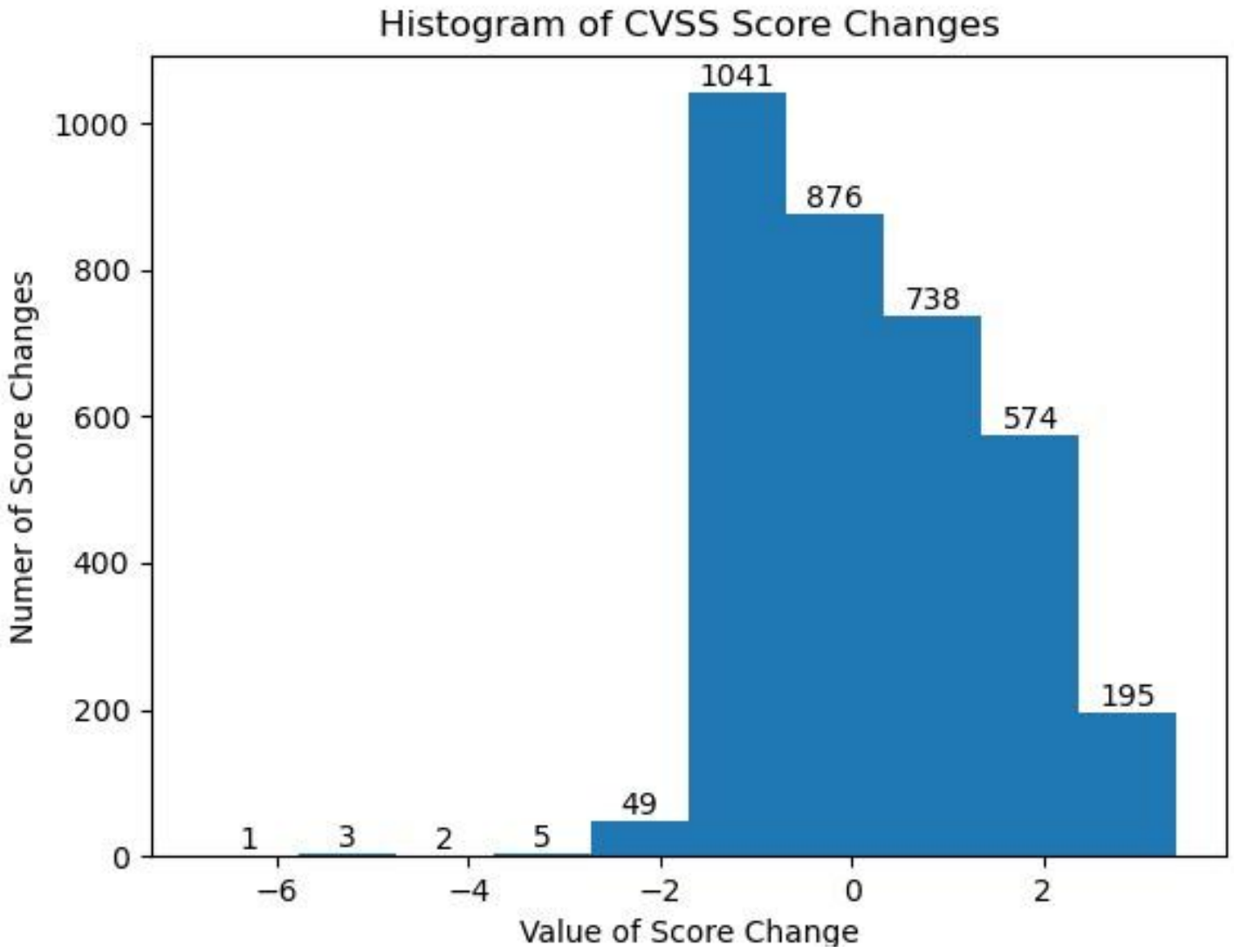
Cisco Study – Public CVEs

- Qualitative boundary shift
  - 15% (49 out of 308)
- Total Increases: 42
  - Low to Medium: 5
  - Medium to High: 36
  - High to Critical: 1
- Total Decreases: 4
  - Medium to Low: 0
  - High to Medium: 2
  - Critical to Medium: 2
- Big shifts: 3
  - Critical to Medium: 3



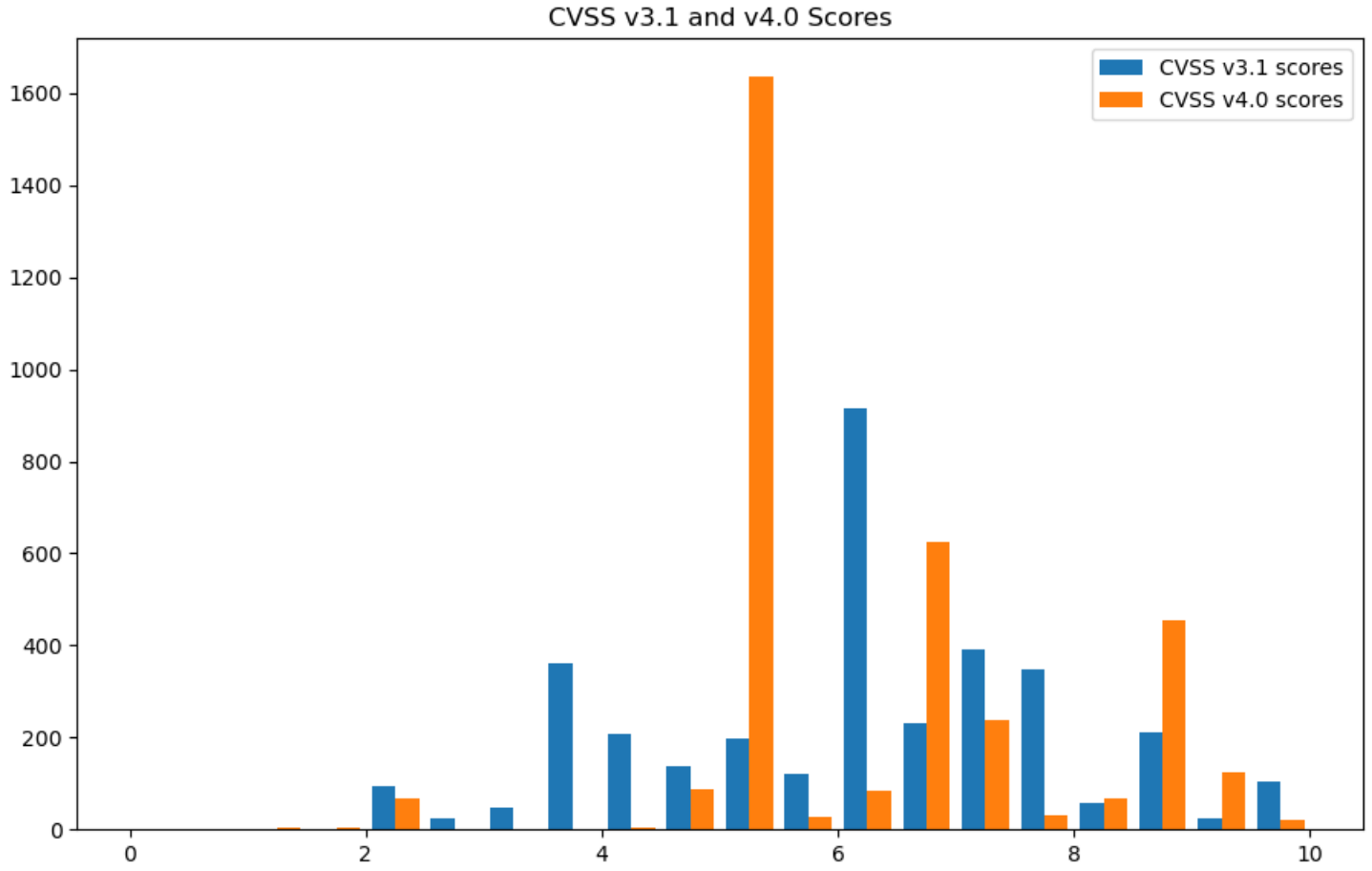
CVE Program

- 3516 records
- Average change
  - 0.19
- Mode
  - -1.0
- Qualitative boundary shift
  - 32% (1111 out of 3516)
- Range
  - Increase: 4.0
  - Decrease: -6.8
  - Total: 10.2



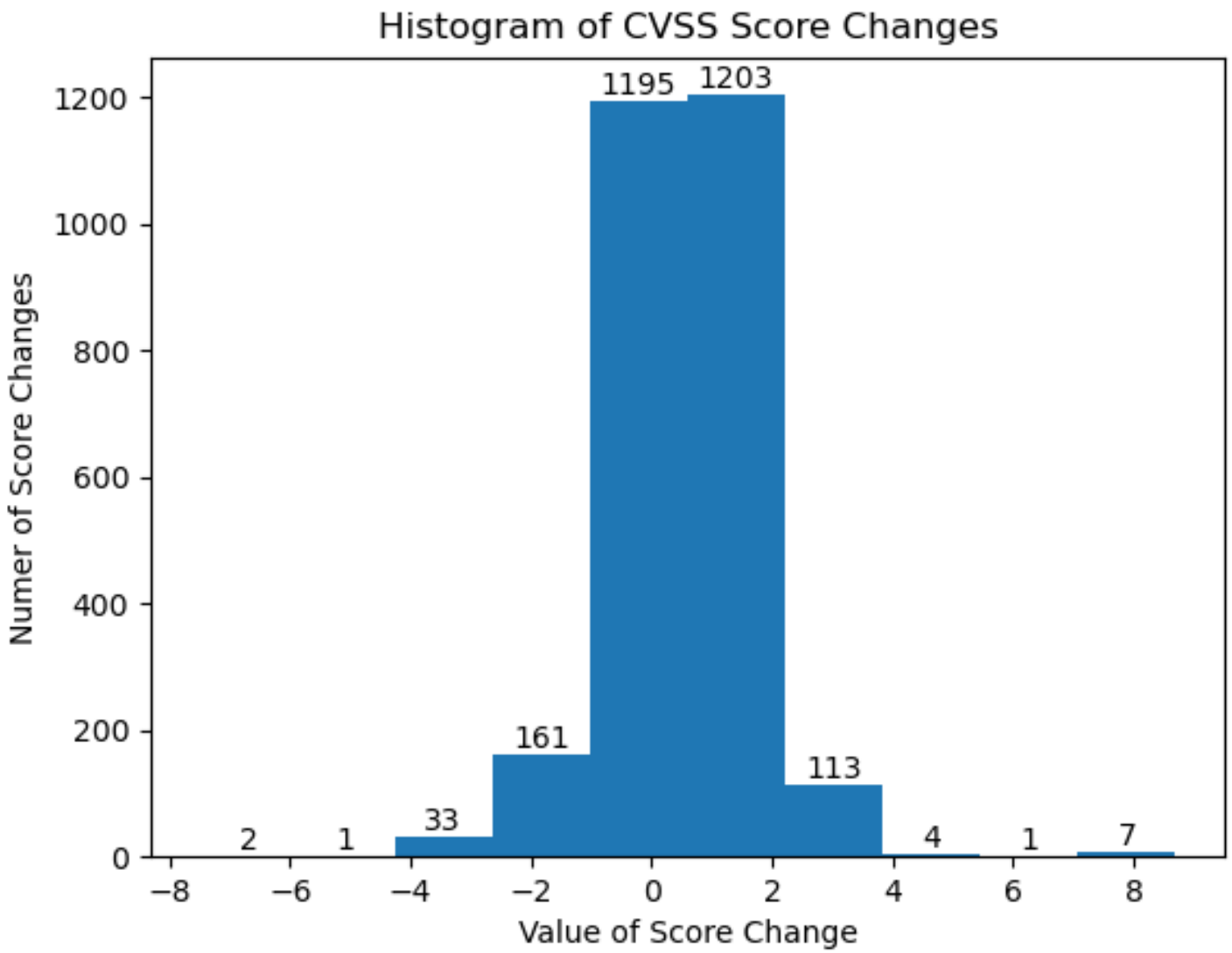
CVE Program

- Qualitative boundary shift
  - 32% (1111 out of 3516)
- Total Increases: 696
  - Low to Medium: 491
  - Medium to High: 164
  - High to Critical: 41
- Total Decreases: 408
  - Medium to Low: 31
  - High to Medium:359
  - Critical to Medium: 18
- Big shifts: 7
  - Critical to Medium: 3



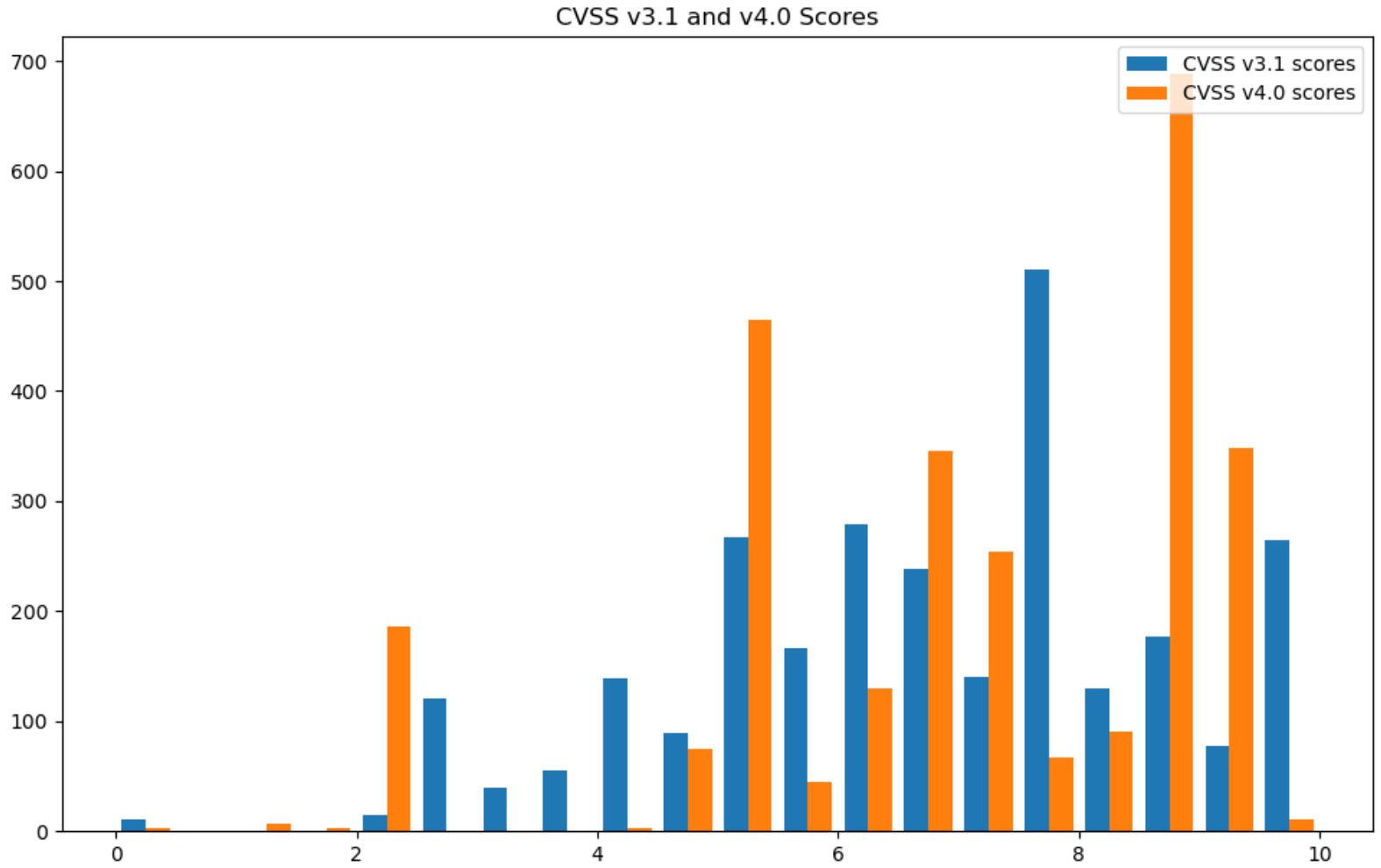
Github Advisories (Reviewed)

- 2720 records
- Average change
  - 0.34
- Mode
  - 1.2
- Qualitative boundary shift
  - 23% (624 out of 2720)
- Range
  - Increase: 8.7
  - Decrease: -7.5
  - Total: 16.2

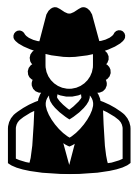


Github Advisories (Reviewed)

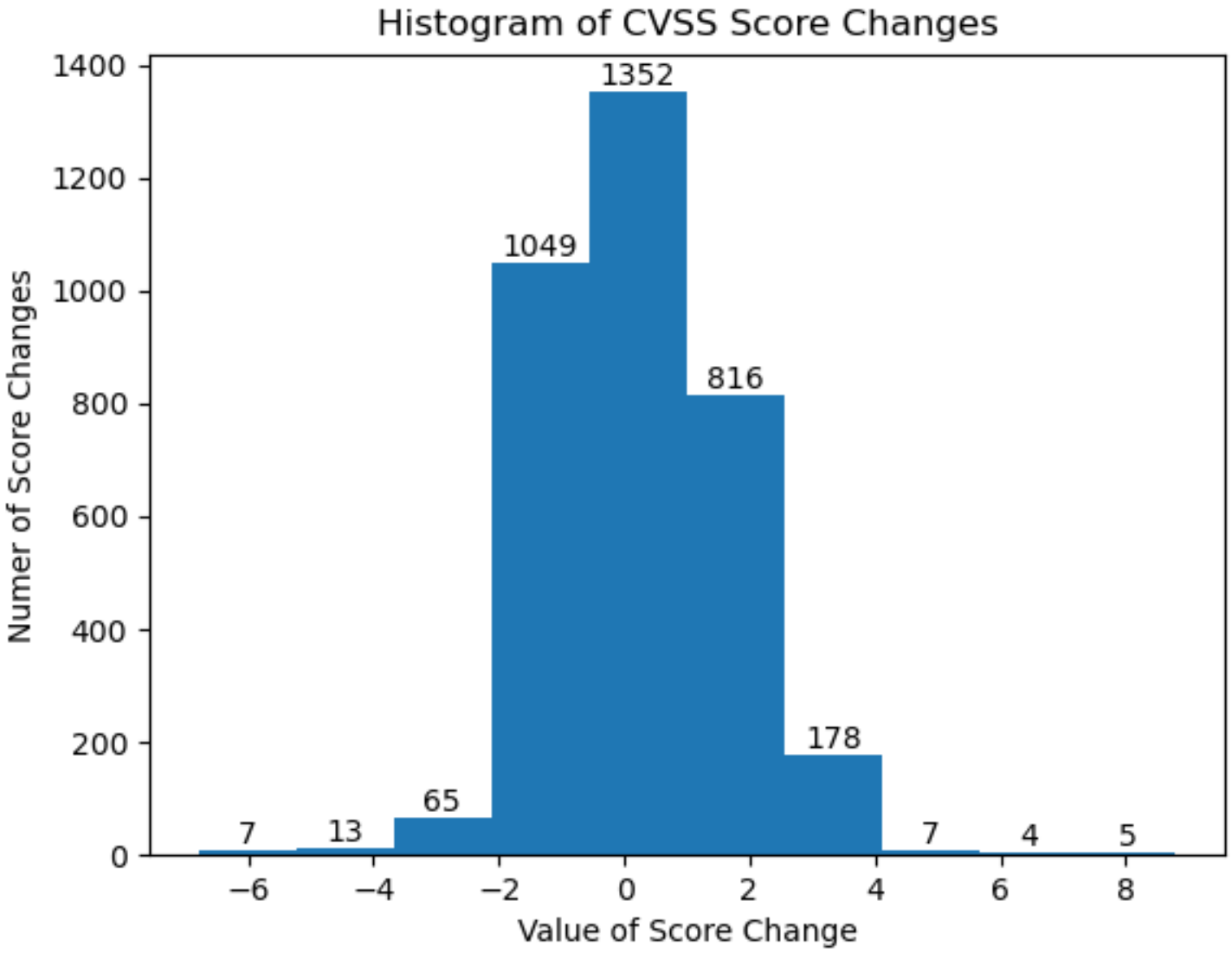
- Qualitative boundary shift
  - 23% (624 out of 2720)
- Total Increases: 411
  - Low to Medium: 71
  - Medium to High: 277
  - High to Critical: 63
- Total Decreases: 191
  - Medium to Low: 35
  - High to Medium: 117
  - Critical to High: 39
- Big shifts: 22
  - Low to High: 7
  - Critical to Medium: 11



GitHub Advisory Data - Unreviewed

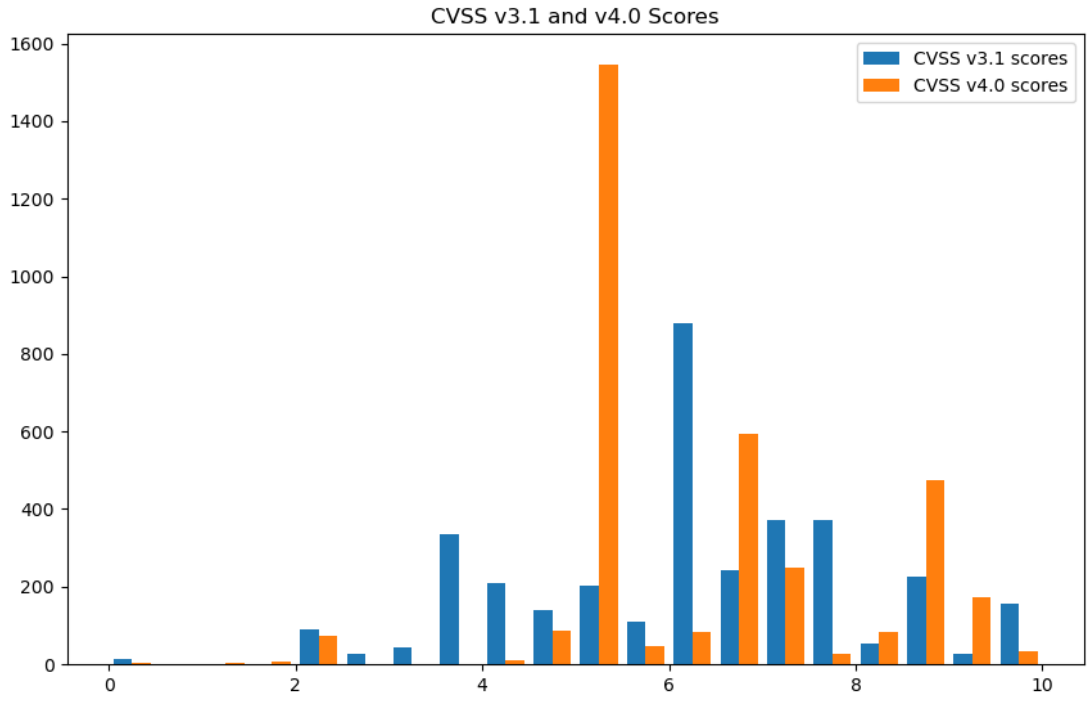


- 3481 records
- Average change
  - 0.19
- Mode
  - -1.0
- Qualitative boundary shift
  - 33% (1151 out of 3481)
- Range
  - Increase: 8.8
  - Decrease: -6.8
  - Total: 15.6



GitHub Advisory Data - Unreviewed

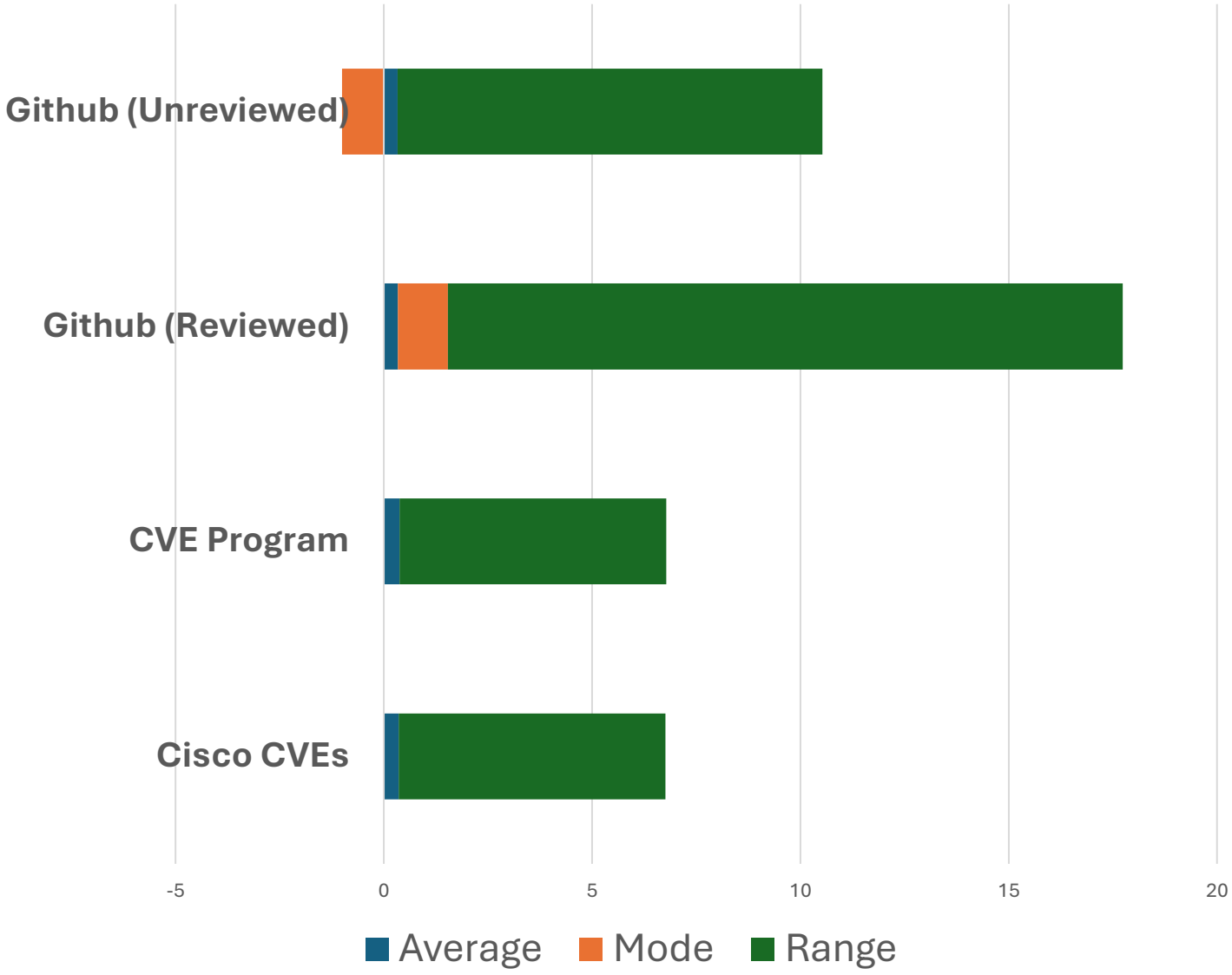
- Qualitative boundary shift
  - 33% (1151 out of 3481)
- Total Increases: 695
  - Low to Medium: 451
  - Medium to High: 185
  - High to Critical: 59
- Total Decreases: 411
  - Medium to Low: 40
  - High to Medium: 342
  - Critical to Medium: 29
- Big shifts: 45
  - Critical to Medium: 21



Data Conclusions

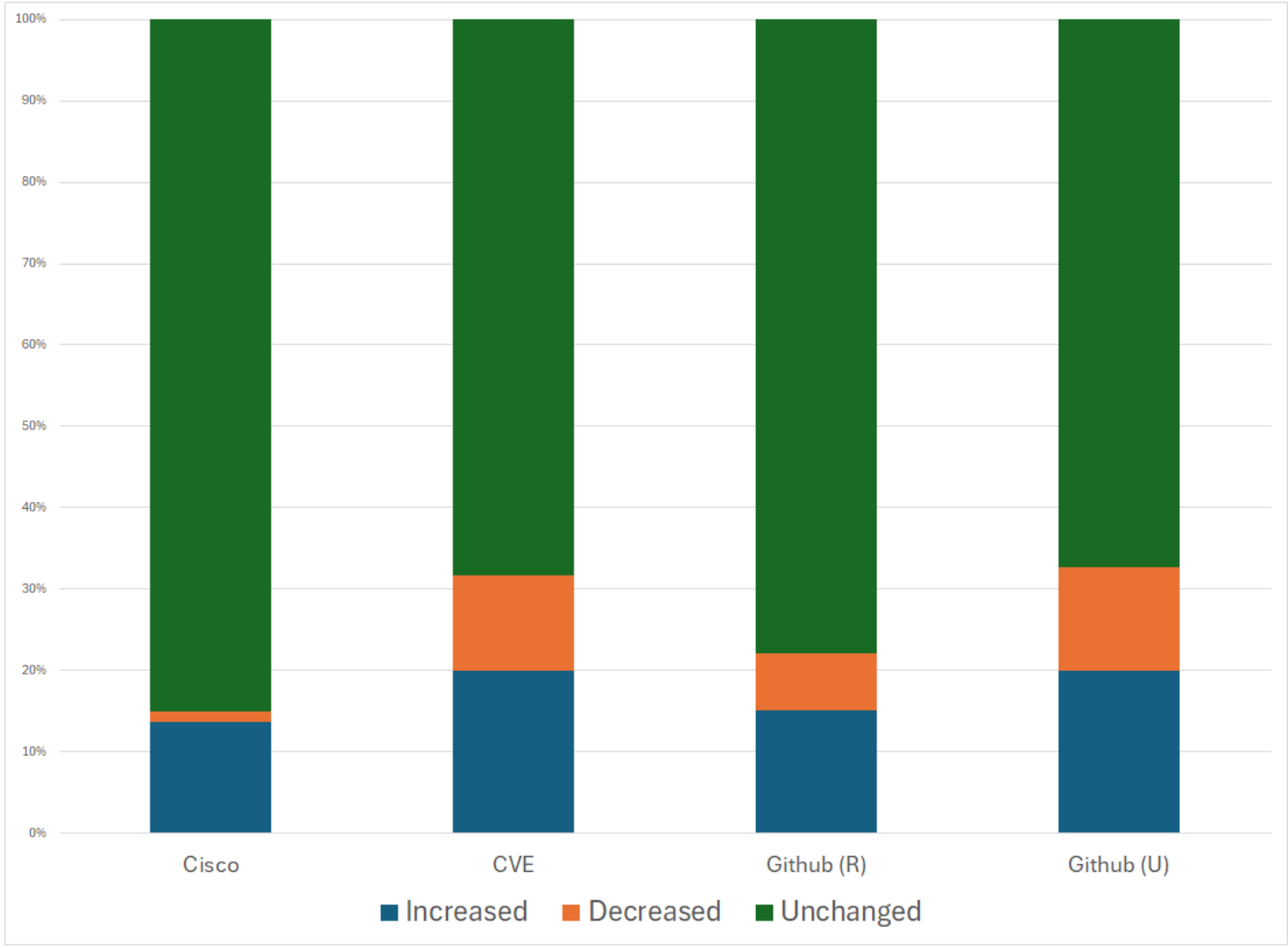
Changes in data sets

- Fairly limited overall changes
- Average changes small (less than 4%)
- Individually, big changes
- Ranges are wide, but likely error-prone



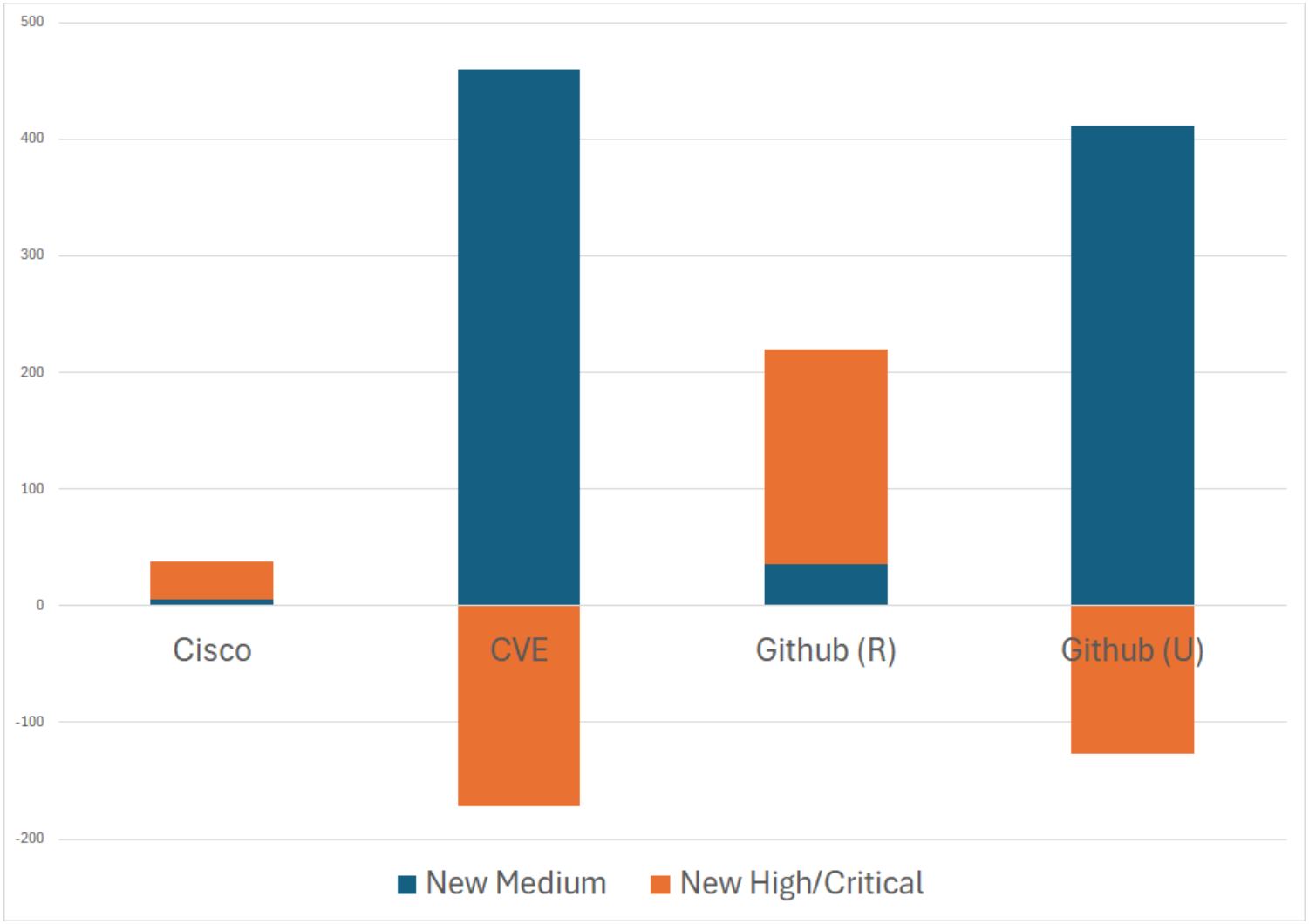
Boundary Changes

- Ratio of entire set
- Represents some big boundary shifts
- Ultimately impacts decision making!



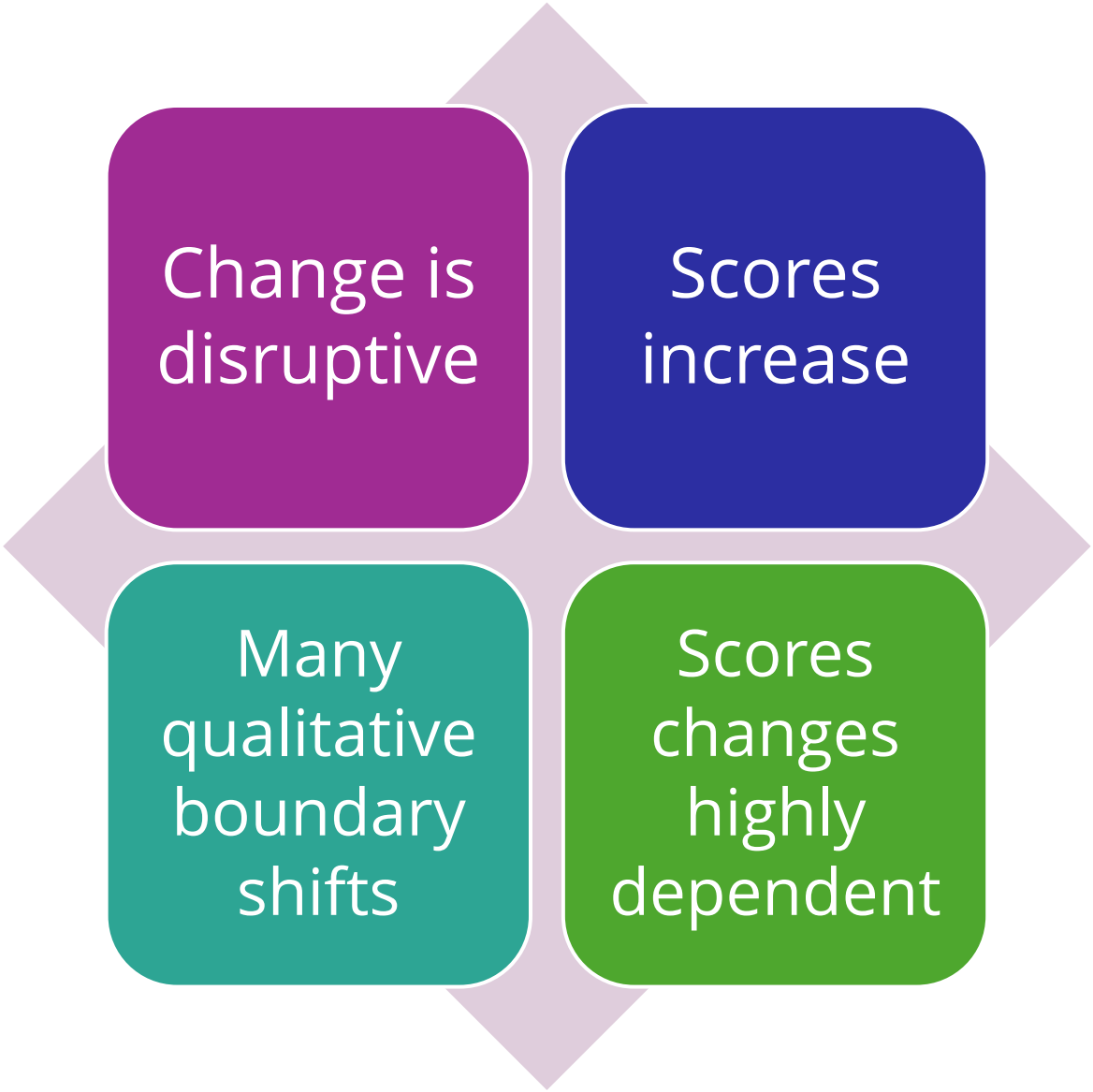
Boundary Changes - Detail

- Marked differences depending on dataset
- More Medium in all sets
- More High/Critical in Github
- Fewer High/Critical in CVE and Github Unreviewed
- Impacts on your use are highly dependent!



CVSS v4.0 Important Takeaways

CVSS v4.0 is Different



What can you do about the numbers?

Producers

- Careful of making promises solely on CVSS Base
- Look more to either full BTE or other identifiers
- Fall back to qualitative ratings
- Your own system, or CVSS Supplemental, or both!

- Use more of the vector string

Consumers

- Careful using only CVSS Base for vulnerability management decisions
- Don’t rely on just CVSS
- Look at EPSS, SSVC, other systems
- Private systems such as Kenna or others

- Use more of the vector string

Resources

- Tools

https://github.com/nickleali/mycvss/blob/main/cvss-comparer/

- SIG contacts

first.org/cvss

first@cvss.org

- The QR code is not a phish
- OR IS IT
- It’s not.

Questions?

Thank you!

FIRST™
Improving Security Together