Vulnerability Prioritization Options

CERT Vendor Meeting

Chris Madden

6 May 2024

Carnegie Mellon University

Software Engineering Institute

About Me

Chris Madden

Yahoo Paranoids Product Security Engineer

Chris has worked as a software engineer and system architect building secure trustworthy software at scale for embedded and cloud for more than 20 years.

He's not big on titles, hierarchy, status quo, or hype.

He's big on analysis and validation and understanding things deeply - using data analysis and dumb questions to build that understanding.

https://www.linkedin.com/in/chrisamadden

yahoo!

Risk is per Asset and depends on the Impact of a Vulnerability being exploited by a Threat

Risk Definition from NIST Special Publication 800-30 r1 Guide for Conducting Risk Assessments

Risk Based Prioritization Context - Content

Risk per Vulnerability

Understanding and Using the building blocks.

[Understanding Your Vulnerability Data To Optimize Your DevOps Pipeline Flow](#) **by Chris Madden, BSides Dublin 2023 with a Taxonomy**

AKA Chris tries to understand Risk and the Vulnerability Management landscape to optimize flow of s/w, and risk.

RBP for the masses

https://riskbasedprioritization.github.io/ **or** riskbasedprioritization.com **March, 2024**

Vulnerability Prioritization Options

Now that we really understand Risk (Exploitation and Impact), let's understand what we do with this info.

Vulnerability Prioritization Options - what data sources to use, and how to prioritize with them, Chris Madden, CERT Vendor Meeting, May 6 2024

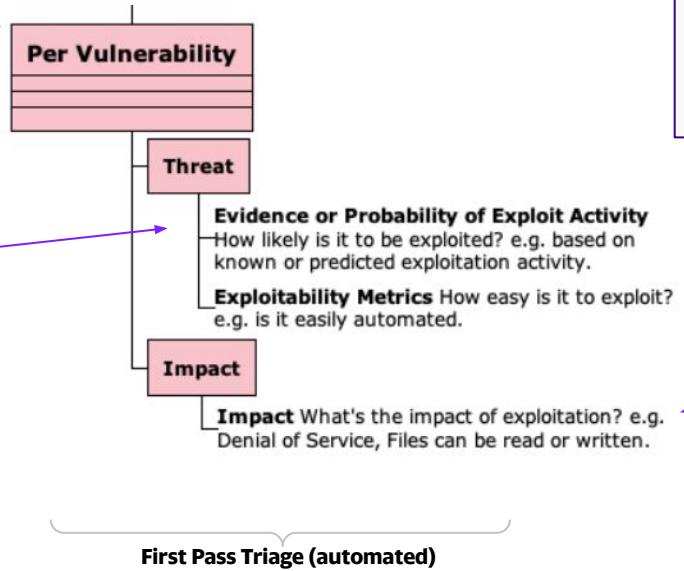
AKA Chris gives a user-centric view of the value of SSVC.

EPSS Likelihood of Exploitation

EPSS for the masses.

Exploit Prediction Scoring System (EPSS) - The User Guide by Chris Madden, BSides Dublin 2024, May 18

AKA Chris tries to help others understand EPSS and how to use it.



Impact

For the subset prioritized by Likelihood of Exploitation, focus on Technical Impacts that are most relevant to you.

Understanding and Using Impact so you know what Vulnerabilities to fix first by Chris Madden, BSides Dublin 2024, May 18

AKA Chris tries to understand the Technical Impact part of Risk, and learns NLP (Natural Language Processing) and LMs (Language Models) to extract the impact text from the 230K published CVEs Descriptions.

Risk is per Asset and depends on the Impact of a Vulnerability being exploited by a Threat

https://github.com/theparanoids/PrioritizedRiskRemediation Risk Definition from NIST Special Publication 800-30 r1 Guide for Conducting Risk Assessments

Why the Content?

The Customer

John Heldreth Author 3w •••

Automotive Security Operations @ Volkswagen AG | Pioneeri...

So... I have been researching this the last few days (maybe weeks) and I need to share with you something... you have to check out this video https://www.youtube.com/watch?v=oMZN810xfck&t=2s Chris Madden's approach is great. Probably not one to one for all industries directly copy paste but the method he goes through, is perfect. I was able to create a prioritization method for Automotive vulnerabilities in an hour or two. Thanks Chris and hope that you will do more good presentations like this one. For everyone else, take the time and watch this... it's worth it.

https://github.com/theparanoids/prioritizedRiskRemediation

Your guide to navigating the treacherous journey of software vulnerabilities and standards to effectively prioritize by Risk

https://riskbasedprioritization.github.io/

Santiago Yepez Crow • 1st 1mo •••

Telecommunication Engineer | Ethical Hacker | Cybersecurity Enginee...

Great job 👏, one of the best things about vulnerability management I have seen!!!

To help me, and other users/practitioners like me

LinkedIn post

LinkedIn post

Why Should I Care?

The Customer

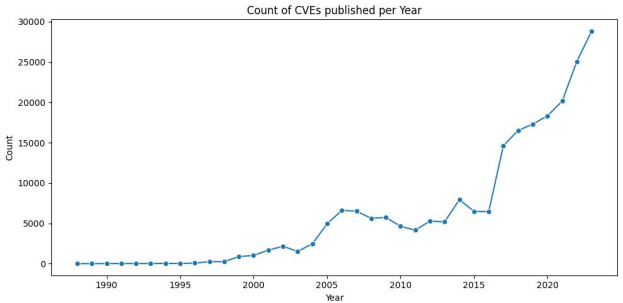
Erik Cabetas • 1st — 1w (edited) •••

Offensive Security leader @Include Security; obsessed w/ Product Se...

I love SEI, they have put out some really good things and have top researchers on their staff. But I just wish they would design their websites and standards in such a way that actually speaks to business stakeholders in a compelling way.

Their website doesn't answer any key questions around need and value. It reads as a "This is what this is" not "This is WHY this is" statement. Since you said you worked on it, perhaps you can lead them in the right direction Patrick Garrity 🍇🛹💙!!

IMHO It should take somebody <1min to read the website of the standard to understand why they should adopt it, what business challenges are solved, and (generally) how much effort it would take to use it.



Problem

- There is an explosion in the number of published CVEs (~100/day)
- Organizations are drowning in a sea of vulnerabilities, not knowing what to remediate first

Currently

- The current industry standard for scoring vulnerabilities (CVSS) does not allow users to effectively prioritize by risk (even if users used it correctly).

Solution

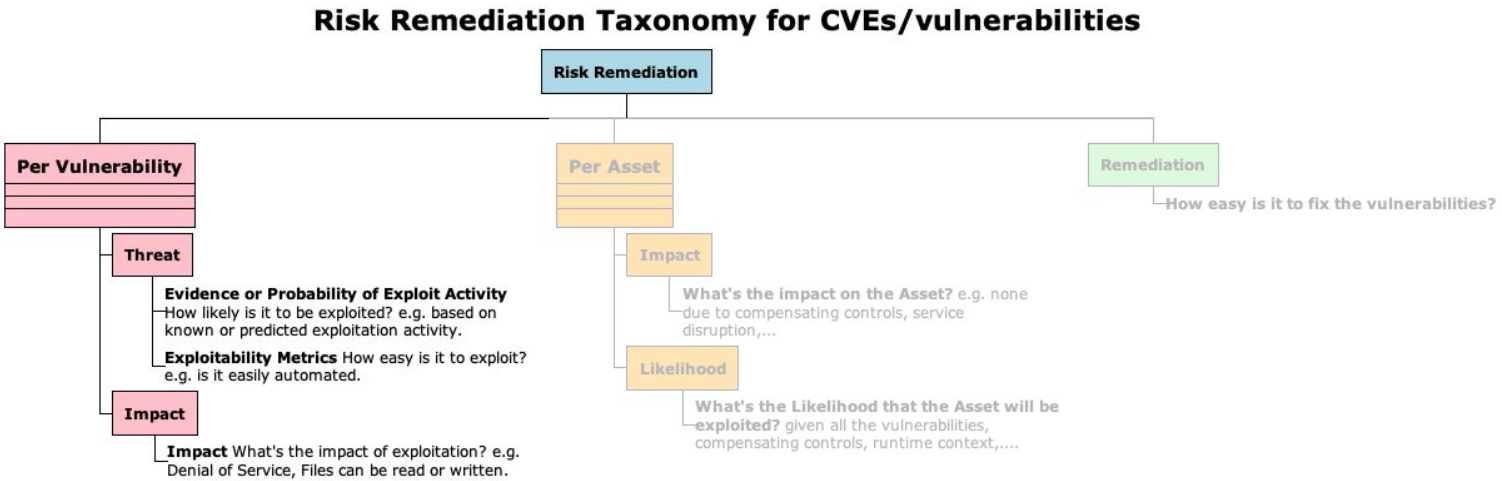
- Prioritizing vulnerabilities
  - by **Exploitation** (as recommended by CISA, Gartner): being exploited in the wild, or are more likely to be exploited, significantly reduces the
    - cost of vulnerability management
    - risk by reducing the time adversaries have access to vulnerable systems they are trying to exploit
  - by **Impact** (as recommended by MITRE) allows for additional independent cost and risk reduction
- **SSVC (Stakeholder-Specific Vulnerability Categorization) Decision Trees** are an effective solution for this prioritization of Exploitation and Impact data in a clear, understandable, and automated way (unlike existing standards) resulting in a significant reduction in cost and risk.

Are you in?

https://cve.icu/CVECalendar.html https://www.first.org/epss/data_stats https://riskbasedprioritization.github.io/risk/Vulnerability_Landscape/ linkedin post

First Pass Triage per Vulnerability

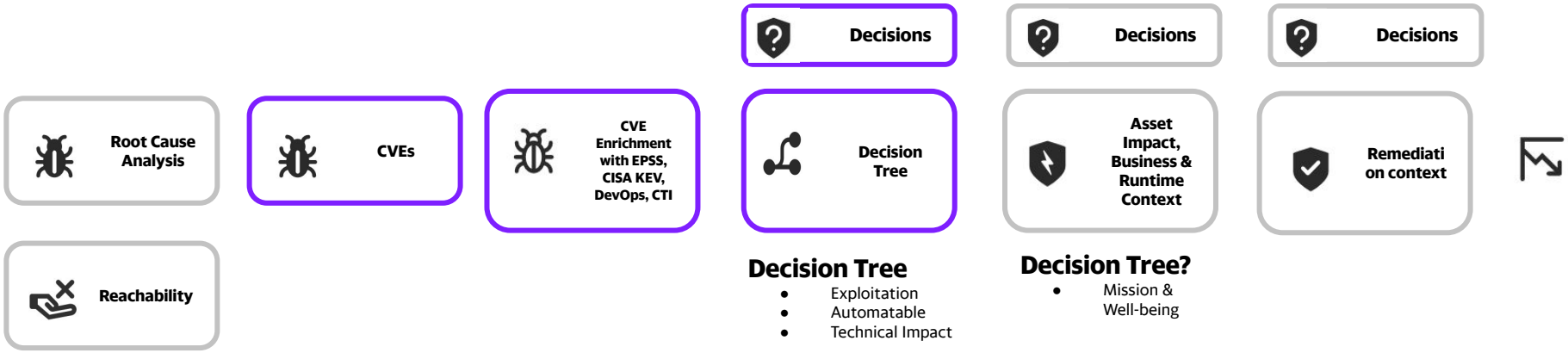
Risk Based Prioritization: Per Vulnerability (CVE)



Mature sciences do a first pass triage (Medical Triage, Financial Analysis,...)

https://github.com/theparanoids/PrioritizedRiskRemediation

Risk Based Prioritization: First Pass Triage



3 R's to address Risk:

1. **Root Cause Analysis**
2. **Reachability**
3. **Risk Based Prioritization**

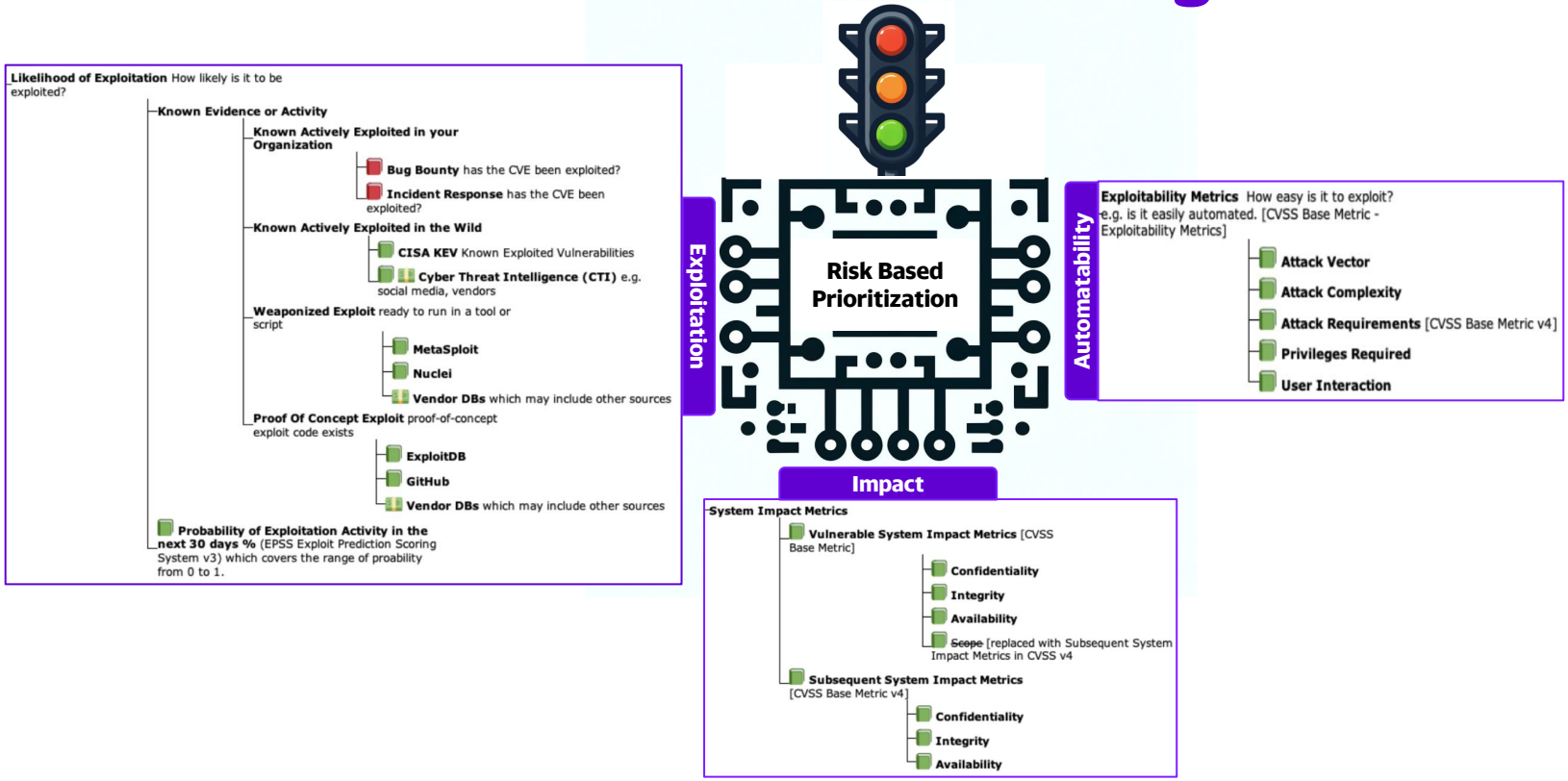
First Pass triage of a CVE can be automated

https://riskbasedprioritization.github.io/organizations/Yahoo/

https://github.com/theparanoids/PrioritizedRiskRemediation

What Data to use in First Pass Triage of Risk

Data Sources to use for First Pass Triage



Risk is per Asset and depends on the Impact of a Vulnerability being exploited by a Threat

https://github.com/theparanoids/PrioritizedRiskRemediation

Exploitation: Exploiting the Asymmetry in the Data

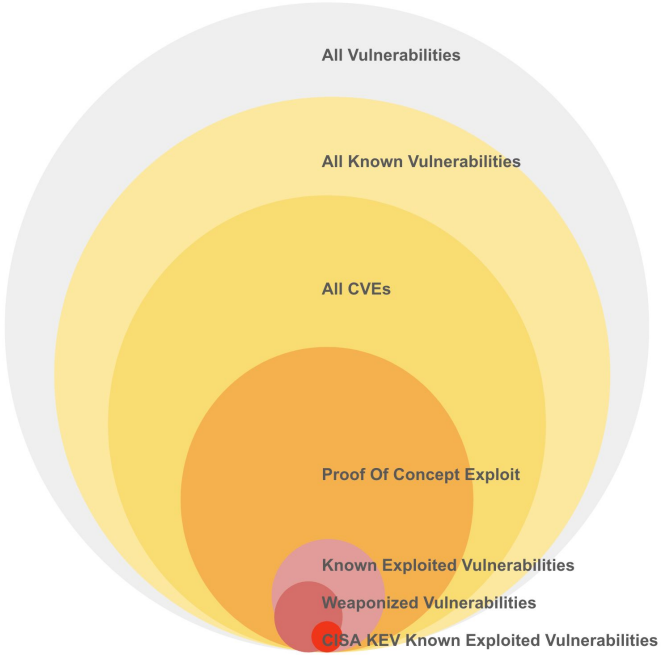
Prioritizing vulnerabilities that are being exploited in the wild, or are more likely to be exploited, reduces the

1. cost of vulnerability management
2. risk by reducing the time adversaries have access to vulnerable systems they are trying to exploit

Our ability to remediate depends on

1. the priority (risk) of CVEs - the ones we want to remediate based on our security posture
2. the number of CVEs for that priority (risk) - that we have the capacity/resources to fix

For prioritization, we can exploit the asymmetry i.e. the number of CVEs decreases significantly with higher evidence or likelihood of exploitation.



Population Sizes associated with the Risk Remediation Taxonomy - Likelihood of Exploitation branch.
Representative sizes and overlaps shown as there isn't authoritative exact data.

Only about 5% or fewer of all CVEs have been exploited

- "Less than 3% of vulnerabilities have weaponized exploits or evidence of exploitation in the wild, two attributes posing the highest risk," Qualys
- "Only 3 percent of critical vulnerabilities are worth prioritizing," https://www.datadoghq.com/state-of-application-security/
- "Less than 4% of the total number of CVEs have been publicly exploited", CISA KEV
- "We observe exploits in the wild for 5.5% of vulnerabilities in our dataset," Jay Jacobs, Sasha Romanosky, Idris Adjerid, Wade Baker

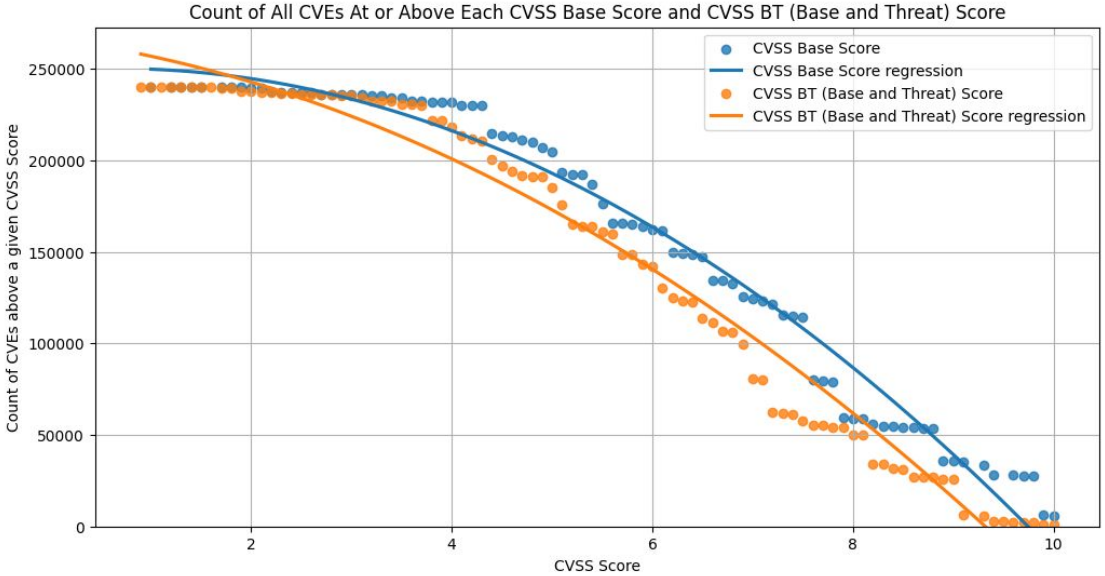
~5% of CVEs are exploited, so prioritize those

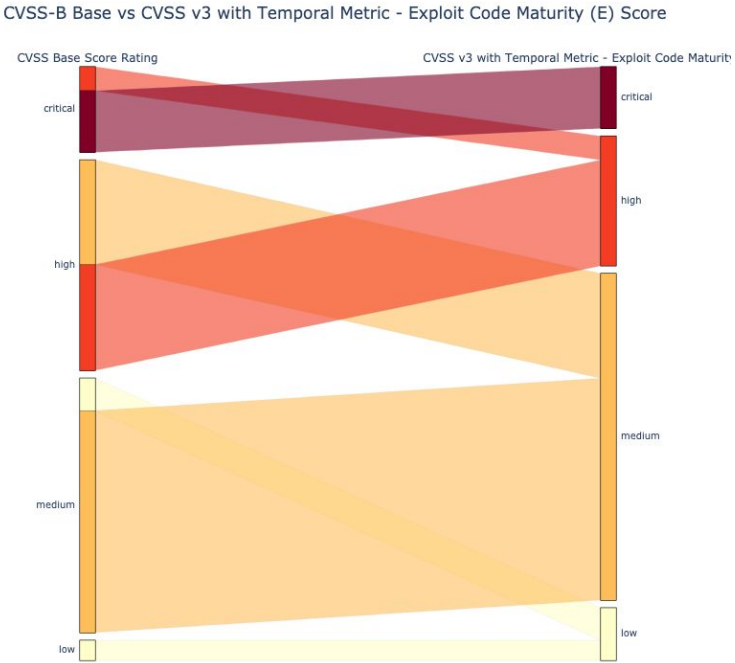
https://riskbasedprioritization.github.io/risk/Understanding_Risk/ https://riskbasedprioritization.github.io/risk/Data_Sources/

How to use this Data for Risk Based Prioritization

CVSS Score and Rating

The convenience of a CVSS Rating, or single CVSS score, comes with the cost of not being able to understand or differentiate between the risk factors from the score, and not being able to prioritize effectively.





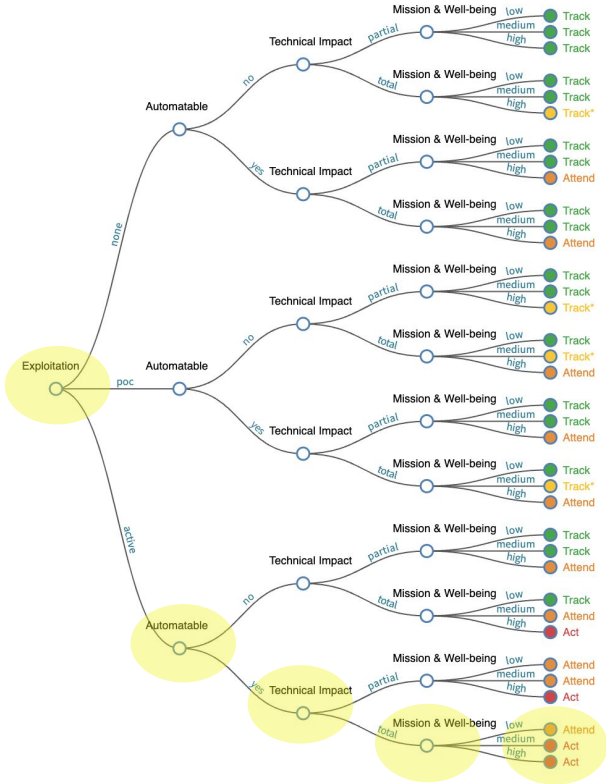
There isn't much granularity for prioritization based on CVSS Score or Rating

https://riskbasedprioritization.github.io/cvss/CVSS/

SSVC Decision Trees

Why Decision Trees?

1. Focus on what matters: risk and its constituent components and what action needs to be taken when
2. Understandable.
3. Modular: e.g. allows change/customization of Mission & Well-being Decision Node for an organization. Loose coupling, high cohesion.
4. Decision Tree Analysis can be applied
5. Trees gives a very clear visual of all the parameters and decision nodes e.g. Attack Trees for Threat Modeling. Formulas are opaque, single output.

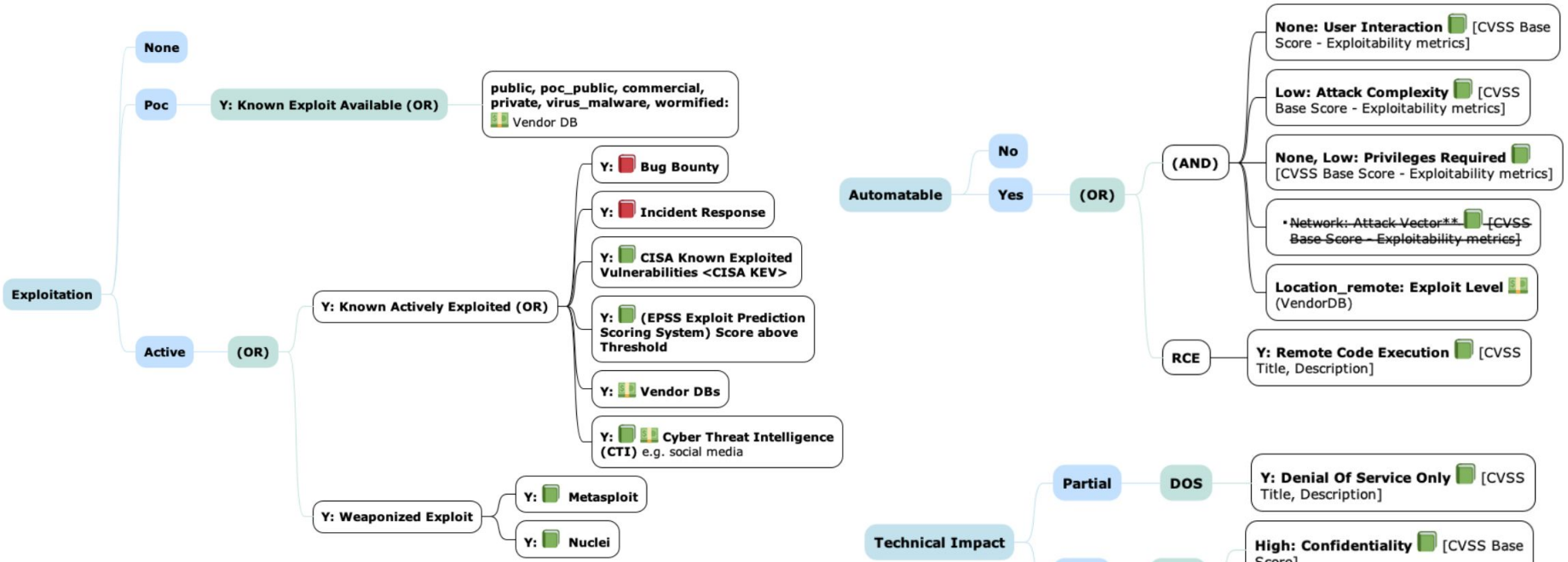


CISA Coordinator Decision Tree

Decision Tree Nodes are the components of risk, with focus on Exploitation

https://riskbasedprioritization.github.io/ssvc/SSVC/

Risk-based Decision Tree Decision Node Inputs



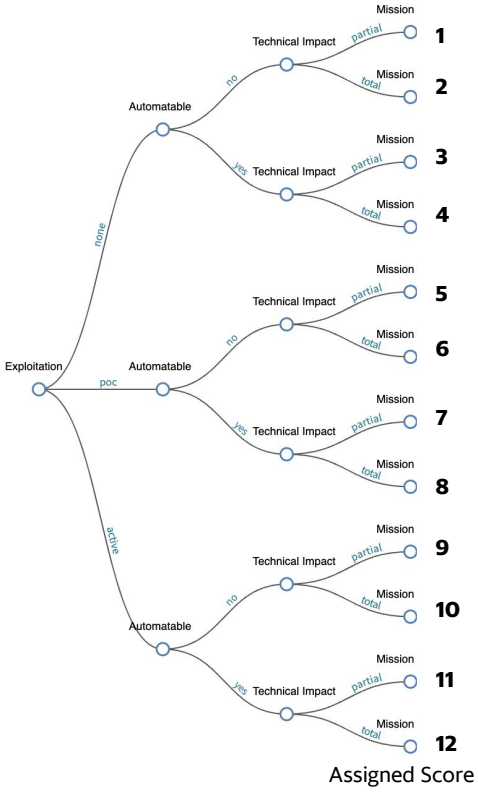
Icon	Description
	Internal
	Open and available to anyone
	Paid product

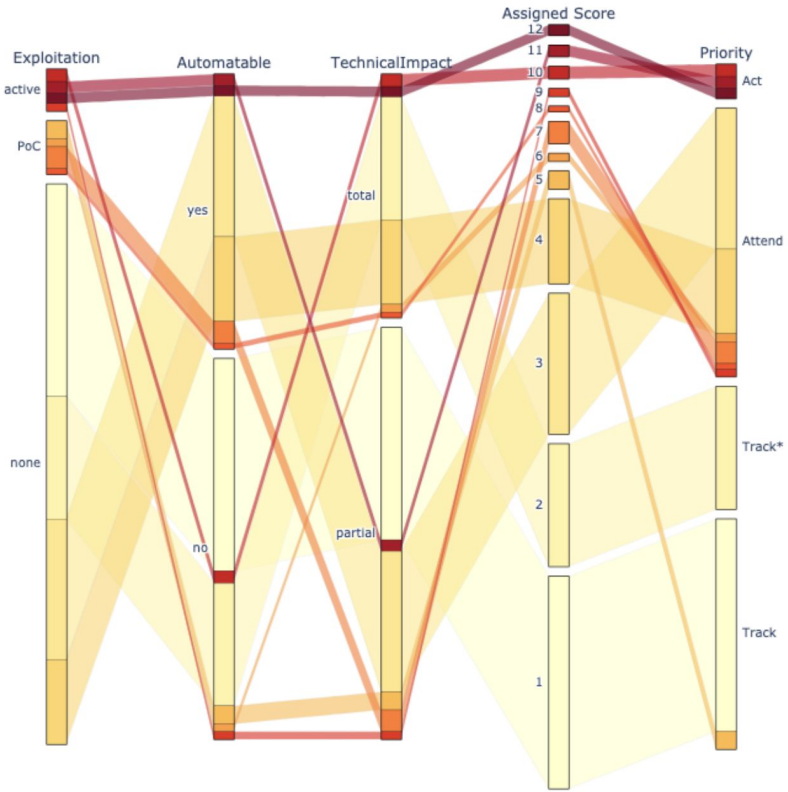
CVSS metrics and other data sources can be used as Decision Nodes Inputs

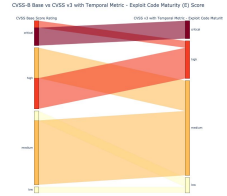
https://riskbasedprioritization.github.io/organizations/Yahoo/

https://github.com/theparanoids/PrioritizedRiskRemediation

Decision Tree for All Published CVEs







CVSS

The Risk Based Prioritization is a lot more granular for what to remediate first

https://riskbasedprioritization.github.io/risk/Rbp_schemes/

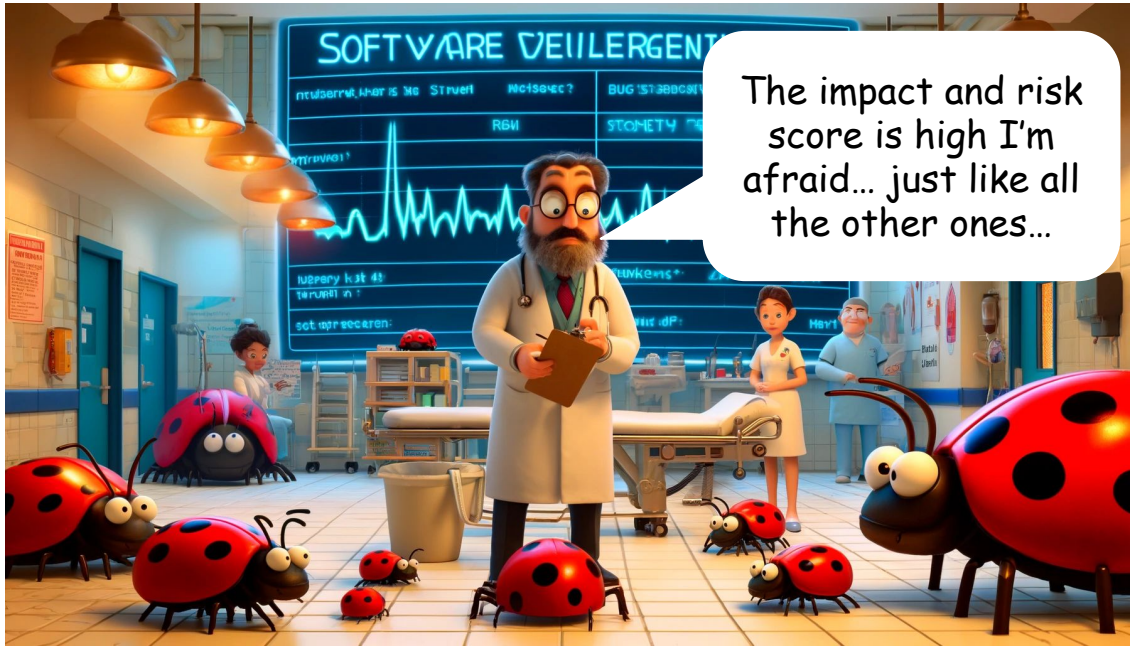
Requirements for a Risk Based Prioritization Scheme for First Pass Triage

1. **Effective Prioritization**
    a. Focus on Exploitation, and include the other Risk Factors
    b. The output (score/rating) should be wedge shaped with the sharp end representing the high risk end i.e. there should be a relatively small number of CVEs at the top end of risk.
2. **Understandable**
    a. The rationale, and preferably the requirements or problem statement, should be stated so it's clear what problem the solution is trying to solve, and the rationale for how it solves it.
    b. Given the output (score/rating), it should be possible to easily and uniquely identify the input parameters(s), and the contribution of the input parameters(s) values to the output.
    c. A non-technical person should be able to understand it
3. **Independent**
    a. Preferably uses Public information
    b. Not dependent on a specific Tool or Vendor or the data from it
        i. Many CTI vendors provide aggregated curated CTI
4. **Extensible**
    a. Organizations may want to extend, customize, or optimize a Risk Based Prioritization Scheme for their environment e.g. change the prioritization associated with a data source or add a new data source.
    b. Some schemes do this by design e.g. *"SSVC aims to avoid one-size-fits-all solutions in favor of a modular decision-making system with clearly defined and tested parts that vulnerability managers can select and use as appropriate to their context."*
5. **Industry Standard**
    a. As users using several solutions, we'd like the risk based prioritization scheme to be standard and interoperable and an industry standard so we have consistent ratings across solutions.

Requirement	CVSS v3 Temporal Metric - Exploit Code Maturity (E)	SSVC Decision Tree
Effective Prioritization	❌	✅
Understandable	❌	✅
Independent	✅	✅
Extensible	❌	✅
Industry Standard	✅	❌

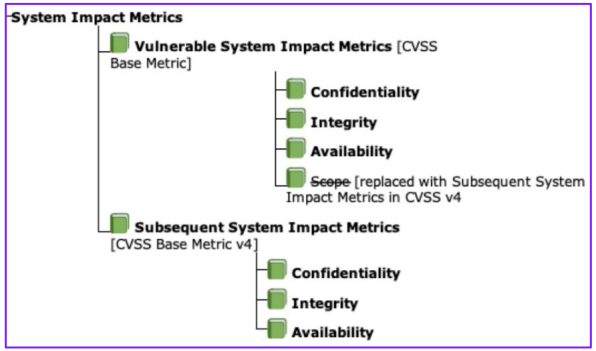
A solution is meaningful in the context of the stated requirements

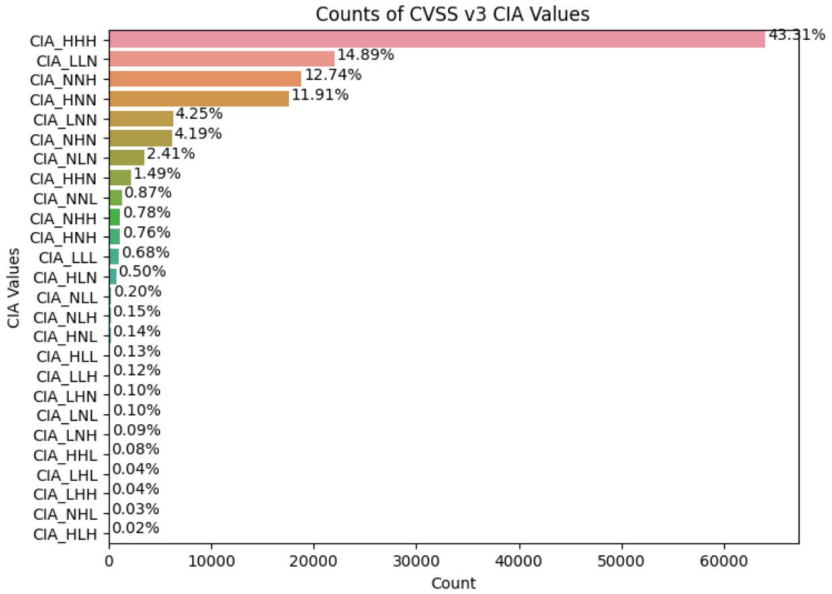
https://riskbasedprioritization.github.io/risk/Rbp_schemes/



But what about the Impact?

CVSS Impact





Counts of Combinations of CIA for CVSS v3 CVEs
e.g. CIA_HHH means that Confidentiality Impact is HIGH, Integrity Impact is HIGH, Availability Impact is HIGH

There isn't much granularity for prioritization based on CVSS Impact values

https://riskbasedprioritization.github.io/cvss/CVSS/

MITRE on Technical Impact

"Software developers often face hundreds or thousands of individual bug reports for weaknesses that are discovered in their code. *In certain circumstances, a software weakness can even lead to an exploitable vulnerability.* ***Due to this high volume of reported weaknesses, stakeholders are often forced to prioritize which issues they should investigate and fix first, often using incomplete information. In short, people need to be able to reason and communicate about the relative importance of different weaknesses."***

Technical Impacts per MITRE

"While there are a large number of weaknesses in CWE, there appear to be ***only eight different consequences or technical impacts*** *to which these failures lead (see the table below). In other words, if a weakness manifests itself in a product in an exploitable manner and an attacker successfully exploits it, then there will be one of eight technical impacts or consequences from that weakness."*

1. Read data — Confidentiality
2. Modify data — Integrity
3. Denial-of-Service: unreliable execution — Availability
4. Denial-of-Service: resource consumption — Availability
5. Execute unauthorized code or commands
6. Gain privileges / assume identity
7. Bypass protection mechanism
8. Hide activities

Impact

Impact Method
(in NIST Vulntology terms)

What should my organization focus on?

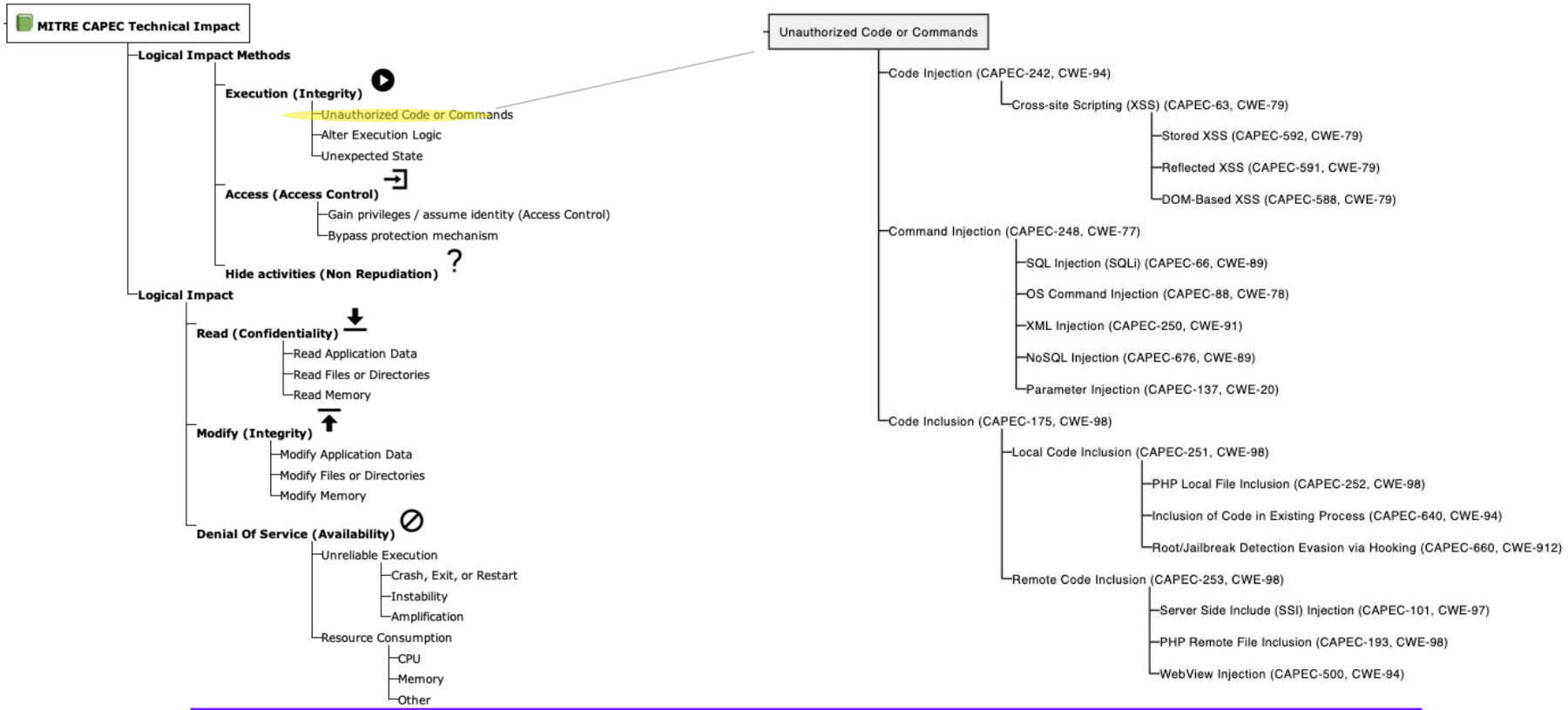
"The collapsing of the hundreds of types of errors into a small set of technical impacts offers a simplification to the question, "What should my organization focus on to gain assurance in our software?".

Instead of trying to remove all weaknesses, you can decide which of the eight impacts are either more or less dangerous to you, given what the software product is doing for your organization."

Using the small number of Technical Impacts allows us to focus on what to fix first

https://github.com/usnistgov/vulntology https://cwe.mitre.org/community/swa/priority.html https://cwe.mitre.org/cwss/cwss_v1.0.1.html

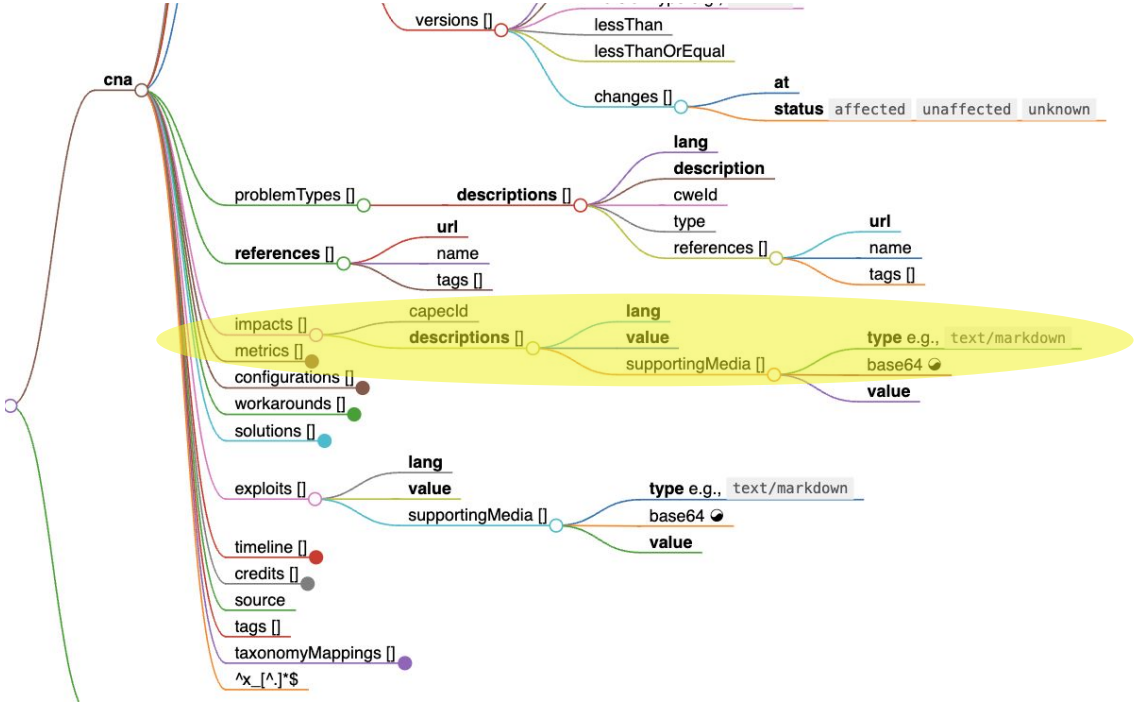
Impact Data To Inform Risk



MITRE Technical Impacts offer different levels of granularity beyond CVSS CIA Impact

CVE Record Format Supports Impact


```
{
  "cnaContainer": {
    "title": "Buffer overflow in Example Enterprise allows
Privilege Escalation.",
    "datePublic": "2021-09-08T16:24:00.000Z",
    "problemTypes": [
      {
        "descriptions": [
          {
            "lang": "en",
            "cweId": "CWE-78",
            "description": "CWE-78 OS Command Injection",
            "type": "CWE"
          }
        ]
      }
    ],
    "impacts": [
      {
        "capecId": "CAPEC-233",
        "descriptions": [
          {
            "lang": "en",
            "value": "CAPEC-233 Privilege Escalation"
          }
        ]
      }
    ],
    "affected": [
      {
        "vendor": "Example.org",
        "product": "Example Enterprise",
        "platforms": [
          "Windows",
          "MacOS",
          "XT-4500"
        ],
```

Impact can be (mostly) represented with a CapecID (Common Attack Pattern)

https://raw.githubusercontent.com/CVEProject/cve-schema/master/schema/v5.0/docs/cnaContainer-advanced-example.json https://cveproject.github.io/cve-schema/schema/v5.0/docs/mindmap.html

CVE Program Encourages CVE Data Enrichment

CVE Program Blog Post April 27 2024

additional vulnerability-related information has become important to the cybersecurity community for increased transparency, enabling vulnerability root cause understanding, and prioritizing incident response*, including* ***CVSS****,* ***CWE****,* ***CPE****, amongst others.*

the authoritative source (within their CNA scope) of vulnerability information — those closest to the products themselves — can accurately report enriched data to CVE directly and contribute more substantially to the vulnerability management process.

Getting more accurate and precise information in the hands of the defenders and downstream customers on a timelier basis helps the vulnerability management ecosystem and the entire cybersecurity community in addressing risks.

More accurate and precise information makes for better decision making

https://medium.com/@cve_program/new-cve-record-format-enables-additional-data-fields-at-time-of-disclosure-82eef1d4035e April 27 2024

Automation Enables Data Enrichment

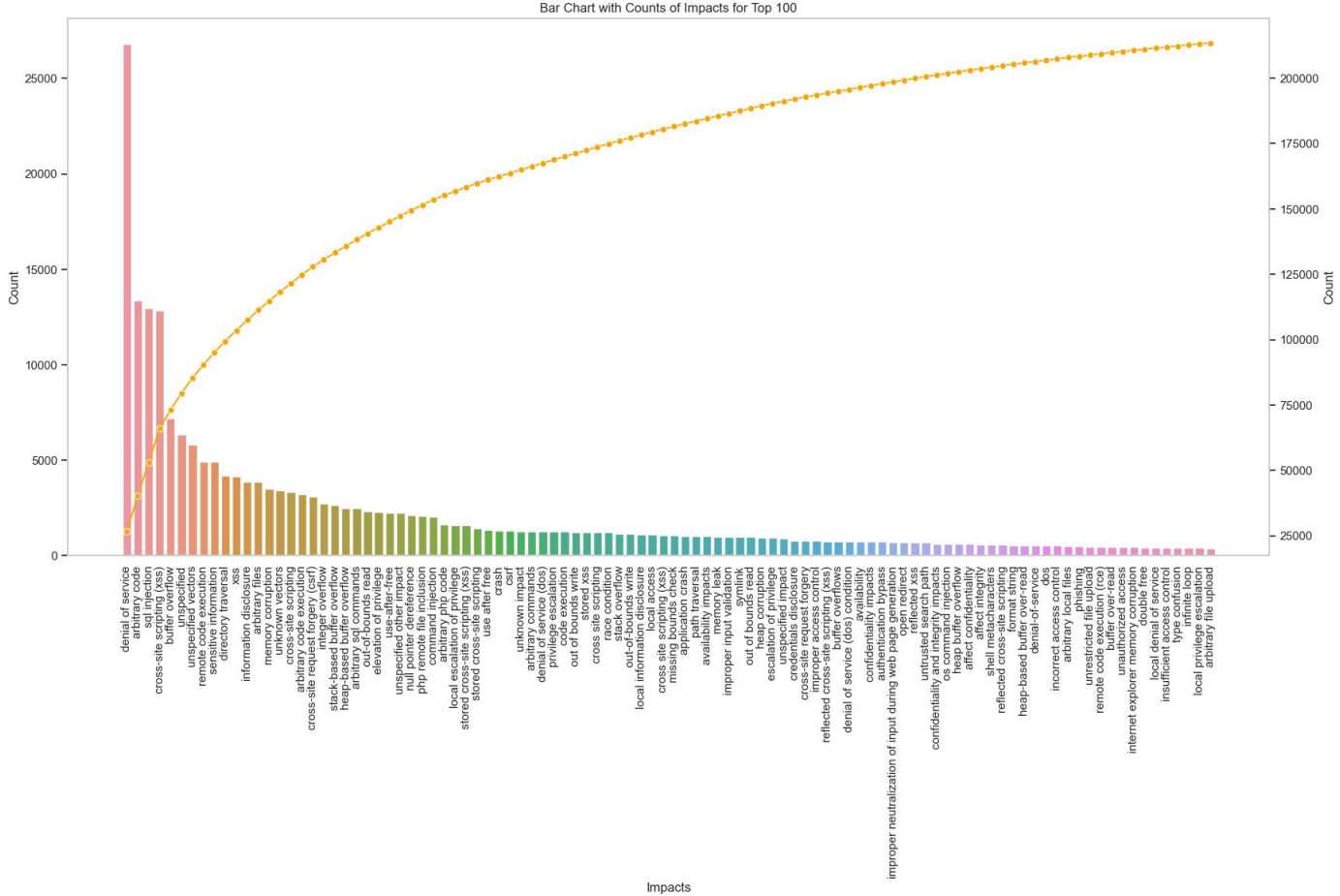
- There is an exponential increase in published CVEs
- There is a reduction in the human resources to process them; recent NVD enrichment disruption
- The tools to process text (Natural Language) have, in the last 3 years, entered a new generation: Language Models
- Yahoo will release
    a. a dataset of the 230K published CVEs with the Impact auto-extracted that can be used to train other models
    b. the details on how to do this

cveID	Description	Extracted Vulnerability/ Impact text	Extracted Vulnerability/Impact text, Start, End, CAPEC Technical Impact, CAPEC ID, CWE ID
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could**execute arbitrary code** with the **privileges of the parent process** (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.	**execute arbitrary code, privileges of the parent process**	[{"value":"**execute arbitrary code**", "start": 100, "end":130, "Impact":"**execute unauthorized code or commands**", "CAPEC":123}, {"value":"**privileges of the parent process**", "start": 150, "end":170, "Impact": "**gain privileges/assume identity**", "CAPEC":123, "CWE":456}]
CVE-2018-15961	Adobe ColdFusion versions July 12 release (2018.0.0.310739), Update 6 and earlier, and Update 14 and earlier have an **unrestricted file upload** vulnerability. Successful exploitation could lead to **arbitrary code execution**.	**unrestricted file upload, arbitrary code execution**	[{"value":"**unrestricted file upload**", "start":100, "end":130, "Impact"**modify files or directories**", "CAPEC":123, "CWE":456}, {"value":"**arbitrary code execution**", "start": 150, "end":170, "Impact": "**execute unauthorized code or commands**", "CAPEC":123}]

Make it easy to add enrichment data - Impact in this case

dummy data shown here

Distribution of Entities Extracted from 230K CVEs



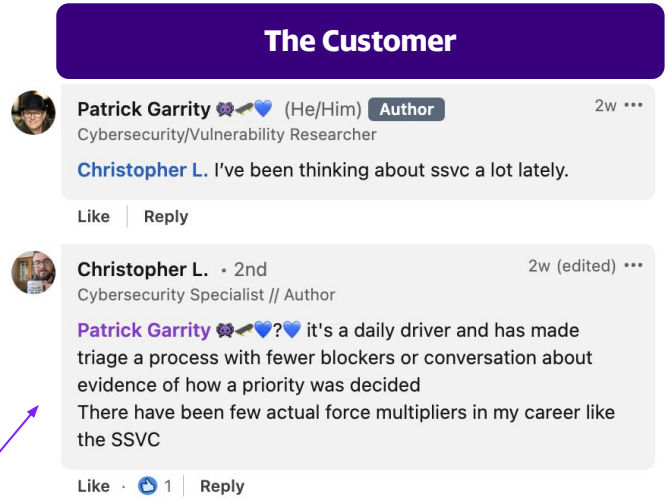
- ~230K CVE Descriptions
- ~37074 unique Entities
- 346027 Entities
- Top 100 unique Entities (100/37047 = 0.3%) account for ~67% (~230K/346027) of all Entities

TakeAways

The TakeAways

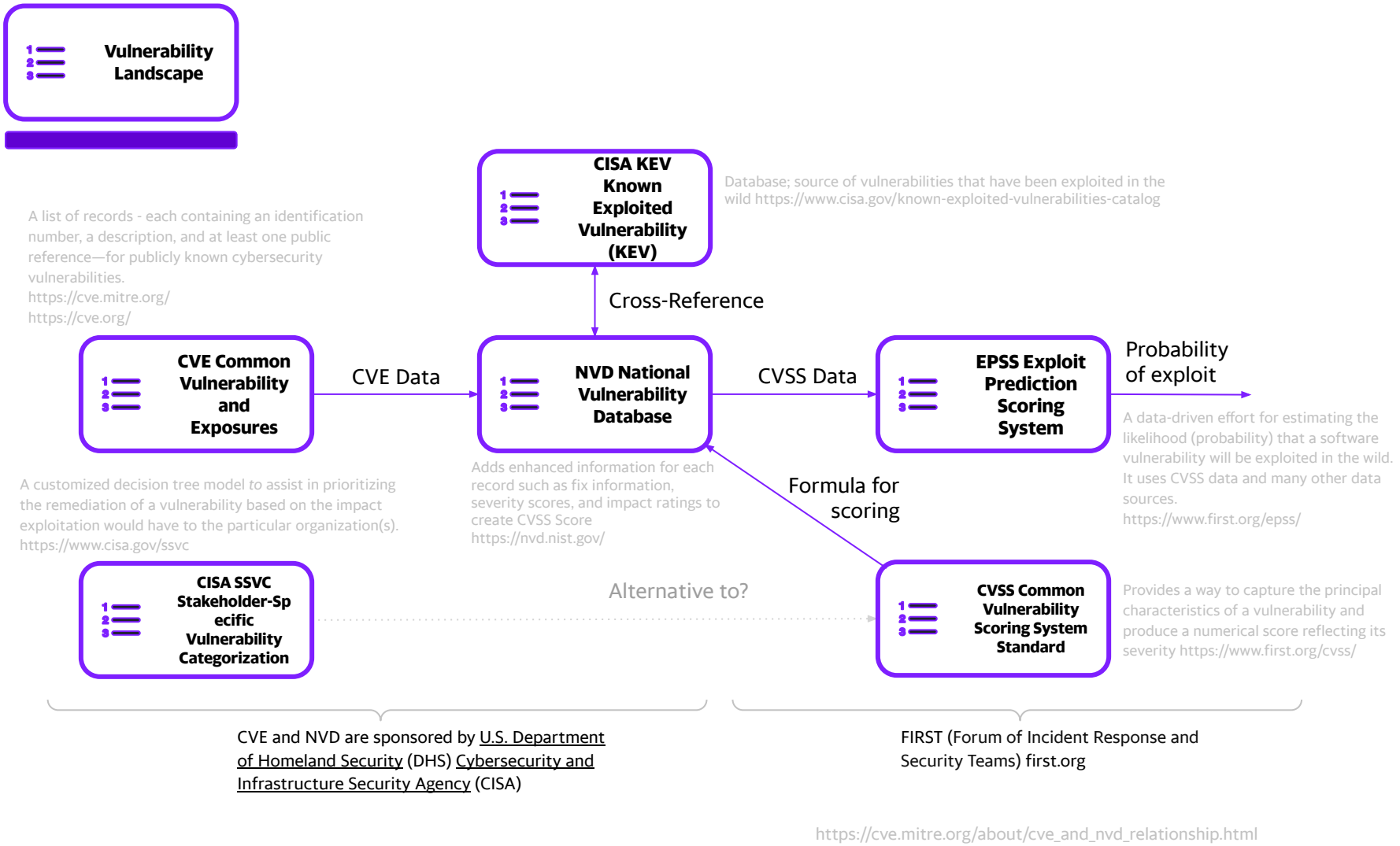
1. **Prioritizing vulnerabilities**
   a. by **Exploitation** (as recommended by CISA, Gartner) i.e. are being exploited in the wild, or are more likely to be exploited, significantly reduces the
      - cost of vulnerability management
      - risk by reducing the time adversaries have access to vulnerable systems they are trying to exploit

   b. by **Impact** (as recommended by MITRE) allows for additional independent cost and risk reduction
2. There is a need for a **Risk Based Prioritization scheme that allows this effective prioritization** that is
   a. **extensible**: that can leverage the rich data available for Risk (Exploitation and Impact) to reduce risk and cost for users
   b. **understandable**: that can be understood by all stakeholders
3. **Additional vulnerability-related information** is available and supported by CVE, and LM technology makes it easier to populate it.
4. **SSVC is uniquely positioned** here to help users.



Thank You!

Annex


Vulnerability Landscape
CISA KEV Known Exploited Vulnerability (KEV)
Database; source of vulnerabilities that have been exploited in the wild https://www.cisa.gov/known-exploited-vulnerabilities-catalog
A list of records - each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
https://cve.mitre.org/
https://cve.org/
Cross-Reference
CVE Common Vulnerability and Exposures
CVE Data
NVD National Vulnerability Database
CVSS Data
EPSS Exploit Prediction Scoring System
Probability of exploit
A data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. It uses CVSS data and many other data sources.
https://www.first.org/epss/
Adds enhanced information for each record such as fix information, severity scores, and impact ratings to create CVSS Score
https://nvd.nist.gov/
Formula for scoring
A customized decision tree model to assist in prioritizing the remediation of a vulnerability based on the impact exploitation would have to the particular organization(s).
https://www.cisa.gov/ssvc
CISA SSVC Stakeholder-Specific Vulnerability Categorization
Alternative to?
CVSS Common Vulnerability Scoring System Standard
Provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity https://www.first.org/cvss/
CVE and NVD are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)
FIRST (Forum of Incident Response and Security Teams) first.org
https://cve.mitre.org/about/cve_and_nvd_relationship.html

Vulnerability Landscape

"CWE is the root mistake, which can lead to a vulnerability (tracked by CVE in some cases when known), which can be exploited by an attacker (using techniques covered by CAPEC)", which can lead to **a Technical Impact (or consequence),** which can result in a Business Impact

- *"CWE focuses on a type of mistake that, in conditions where exploits will succeed, could contribute to the introduction of vulnerabilities within that product."*
- *"A vulnerability is an occurrence of one or more weaknesses within a product, in which **the weakness can be used by a party to cause the product to modify or access unintended data, interrupt proper execution, or perform actions that were not specifically granted** to the party who uses the weakness."*

Vulnerability

Log4 Shell

CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CWE-20, CWE-502

CWE-400

CVE-2021-44228

Inject Unexpected Items

Remote Code Execution to read confidential data

Crypto miners, ransomware, backdoors,...

Weakness, Mistake —(can lead to a vulnerability)→ **Vulnerability** —(which can be exploited by an attacker)→ **Exploit** —(which can lead to)→ **Technical Impact** —(which can result in)→ **Business Impact**

Standard

CWE Common Weakness Enumeration

A community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
https://cwe.mitre.org/

CVE Common Vulnerability and Exposures

A list of records - each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
https://cve.mitre.org/
https://cve.org/

CAPEC Exploit Techniques

Understanding how the adversary operates is essential to effective cybersecurity. CAPEC helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.
https://capec.mitre.org/

???

???

?
Common Weakness Scoring System (CWSS)
https://cwe.mitre.org/cwss/cwss_v1.0.1.html
2014

from MITRE.org

As a user/defender, I care most about these