

Exploit Prediction Scoring System (EPSS) - The User Guide

18 May 2024

<https://www.bsidesdub.ie/>



About Me



Chris Madden

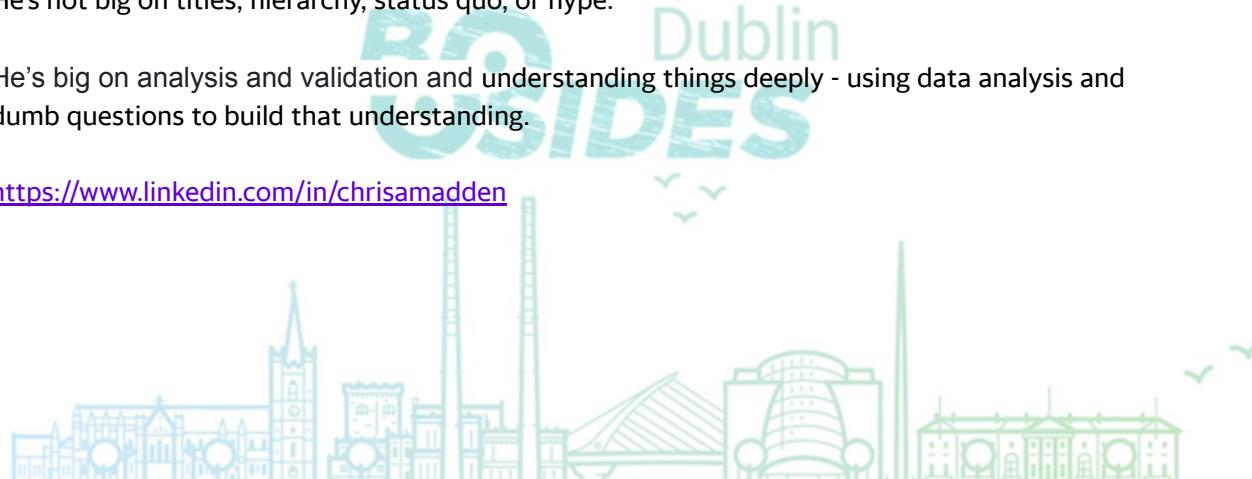
Yahoo Paranoids Product Security Engineer

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>



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

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.

EPSS Likelihood of Exploitation

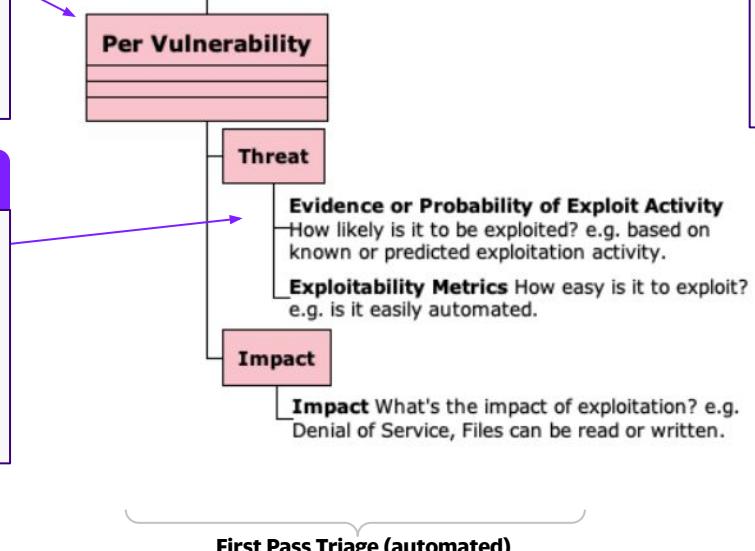
EPSS for the masses.

[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.

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.

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.

Slides here:

<https://riskbasedprioritization.com>

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

Why the Content?

The Customer



John Heldreth **Author**

Automotive Security Operations @ Volkswagen AG | Pioneeri...

3w ...

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/the paranoid s/prioritizedRiskRemediation>

➤ To help me, and other users/practitioners like me

[LinkedIn post](#)

Abstract

Exploit Prediction Scoring System (EPSS) - The User Guide

Exploit Prediction Scoring System (EPSS) is a powerful capability to help organisations prioritise vulnerabilities based on their likelihood of exploitation.

- EPSS is free and publicly available, and there's growing support for it in vendor tools.
- But most users and vendors don't know how to use it.

As a user, I wanted to understand how to use it.

- So I volunteered to work with the EPSS creators to write the guide from a user's point of view.
- The Guide was released March 2024 <https://riskbasedprioritization.github.io/>

In this talk, you'll learn:

- **to understand where EPSS fits in the overall Risk picture**
- **how to use it and why**
- **how others are using it**

This is a follow on to:

- <https://riskbasedprioritization.github.io/> Guide released March 2024
- the BSides 2023 “[Understanding your vulnerability data to optimize your DevOps pipeline flow](#)” talk, where the [overall Risk picture](#) was developed and a Risk Based Prioritization scheme was implemented (that prioritized by Likelihood of Exploitation)

The Guide Launch



Chris Madden · You
Distinguished Technical Security Engineer
1mo ·

On behalf of all those who contributed, I'm excited to share...

👉 Your guide to navigating the treacherous journey of software vulnerabilities and standards to effectively prioritize by Risk: <https://lnkd.in/ebpnQXhc> 🎉

💡 Focusing on exploitation information to prioritize vulnerabilities can dramatically reduce both your risk and effort.

💡 This guide not only dives into the relevant standards and data sources, but also demonstrates how to apply them effectively as part of your organization's Risk-Based Prioritization strategy to significantly reduce:

- The cost associated with vulnerability management.
- The risk by reducing the window of opportunity for adversaries.

👉 Catch Me Live at BSides Dublin! - I'm excited to delve deeper into this topic in my upcoming talk on May 18. For those who can't join in person, stay tuned for the session to be uploaded on YouTube.

😊 Happiness is: working on something you enjoy, with people you admire and learn from!

#Cybersecurity #RiskManagement #VulnerabilityManagement, Security BSides Dublin

Aruneeesh Salhotra, Buddy Bergman, Casey Douglas, Denny Wan, Eoin Keary, Jay Jacobs, Jeffrey Martin, Jerry Gamblin, Jonathan (Jono) Spring, Joseph Manahan, Maor Kuriel, Patrick Garrity Francesco Cipollone, Sasha Romanosky, Stephen Shaffer, Steve Finegan, Chris Lindsey, Toni Ferrara, Sean Poris, Yotam Perkal



➤ The Guide was launched/socialized end of March 2024

[LinkedIn post](#)

The Guide Feedback



Helen McLeish • 3rd+
Chief Cybersecurity Officer
1mo •

Off to update our process doco, it will be much shorter: Read and do this 👍



Chris Madden • 3rd+
Distinguished Technical Security Engineer
1mo •

On behalf of all those who contributed, I'm excited to share...

👉 Your guide to navigating the treacherous journey of software vulnerabilities and standards to effectively prioritize by Risk: <https://lnkd.in/ebpnQXhC> 🎉

+ Follow ...

+ Follow



Santiago Yepez Crow • 1st
Telecommunication Engineer | Ethical Hacker | Cybersecurity Enginee...
1mo ...

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



Chris Hughes • 1st
President @ Aquia | Cyber Innovation Fellow @ CISA | Chief...
[View my blog](#)
1mo • Edited •

...

Risk-Based Vulnerability Management

If you're looking for a comprehensive guide to performing risk-based vulnerability management, you're in luck.

This guide from **Chris Madden** goes into great detail and provides accompanying resources to do just that.

I was pleasantly surprised as I was reading it to see my books "Software Transparency" and "Effective Vulnerability Management" cited as additional resources.

Definitely give this guide a look if you want to learn more about effective vulnerability management, including enrichment and prioritization.

<https://lnkd.in/eJE2s3W8>

#cybersecurity #ciso #vulnerabilitymanagement

Feedback was good

[LinkedIn post](#)

[LinkedIn post](#)

[LinkedIn post](#)



How did that happen?

Deliver Value



Chris Madden 9:39 PM

thanks Jay,

Please add me to the interoperability mailing list.

FWIW my general value-add as a techie is being able to break big things down into small increments of value and deliver on those iteratively - and do so in a way that gets people what they want (aka Lean Agile) aka getting things done.

Generally what works is to

1. define a list of things we want to do - the backlog
2. prioritize the backlog based on value and effort (aka Weighted Shortest Job First) and consensus
3. Get real customers involved in the discussion early aka Turn those affected into those involved.
 - a. That's why I got 2 vendors involved - and they're willing to bring their (anonymized) data to the table/guide
4. Add details to the top items in the backlog only
5. Deliver on these within a defined short time frame
6. Iterate on this

We plan out the big items for the quarter - then break down those big items into deliverable per 2 week periods.

This is all standard Agile stuff - though we don't need to mention Agile when presenting this approach.

...and before anything is done, plan a webinar to present the result 6 months later.

- End of March: Private webinar with Jay Jacobs (creator of EPSS) to coincide with the launch date.
- Mid May: Public conference + YouTube aka submit as a talk for BSides Dublin

▶ **Lean-Agile: I wish I knew this at the start of my career!**

<https://github.com/orgs/RiskBasedPrioritization/projects/1/views/1>

Customer Focus

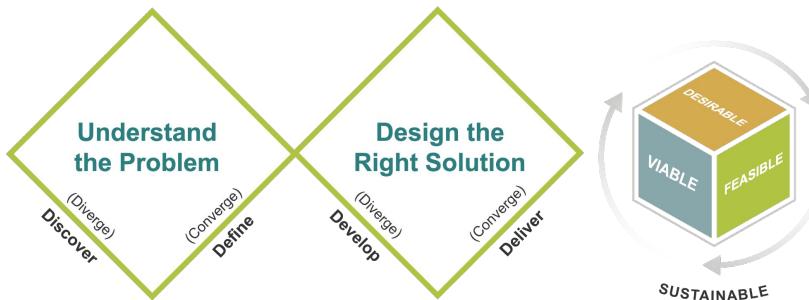
Overview

Any solution should be informed by what the user wants, and the rationale behind the solution implementation. This allows understanding and validation of the solution against the requirements and rationale.

In this section, we look at users' requirements as expressed as User Scenarios and User Stories

Note

The first step of this Guide was asking users that represent stakeholders/roles to provide their requirements as ([User Scenarios](#) and [User Stories](#), and to introduce the [Design Thinking](#) process. Extracts are provided below from [User Scenarios and User Stories](#).



© Scaled Agile, Inc.

User

Security Manager - Get teams to focus on the real issues

Background: CVEs provide a standardized way to identify and track security vulnerabilities across software, services, hardware, SaaS, APIs, etc. CISOs use CVEs to assess the level of risk associated with specific vulnerabilities. The number of CVEs typically indicate the overall security landscape and help prioritize which vulnerabilities should be addressed first.

Pre-Narrative *(how things are now)*

CISOs are constantly subject to allocate their limited resources effectively. Knowing the number of CVEs on hand helps them determine where to focus their efforts. High-severity vulnerabilities with a large number of reported CVEs may take precedence over others, as they pose a greater risk.

The greater the organization, the more complex the situation gets.

If this is not enough, CISOs and directs constantly have a battle with Business, Engineering, Applications teams to provide evidence why a CVE needs to be fixed. Existing scoring like CVSS3 having limitations. Although bigger organizations have access to Threat Intel where CVSS can be married to the threat intel feeds, but this is usually a pipe dream for SMBs or organizations with reduced security budgets.

Post-Narrative *(how we want things to be in the future - aspirational)*

Taking EPSS along with Business Context into account will really help organizations to sift through the CVEs. Focus from VM and Applications teams can be tailored towards fixing the most critical of issues. This will also help with the conversation with Business and App Teams, and reduce (if not eliminate) friction between Security and non-security Teams.

Design Thinking. Get Customers to write user scenarios/stories at the beginning.

<https://scaledagileframework.com/design-thinking/>

Writing Style

The "writing style" in this guide is succinct, and leads with an opinion, with data and code to back it up i.e. data analysis plots (with source code where possible) and observations and takeaways that you can assess - and apply to your data and environment. This allows the reader to assess the opinion and the code/data and rationale behind it.

Different, and especially opposite, opinions with the data to back them up, are especially welcome! - and will help shape this guide.

” Quote

If we have data, let's look at data. If all we have are opinions, let's go with mine.

Jim Barksdale, former CEO of Netscape

About this Guide

About this Guide

This Risk Based Prioritization Guide is a pragmatic user-centric view of [Relative Risk per Vulnerability](#), the related standards and data sources, and how you can apply them for an effective [Risk Based Prioritization](#) for your organization.

It is written by, or contributed to, some of the thought leaders in this space **for YOU**.

[CISA](#), [Gartner](#), and others, recommend focusing on vulnerabilities that are known-exploited as an effective approach to risk mitigation and prevention, yet very few organizations do this.

Maybe because they don't know they should, why they should, or how they should? This guide will cover all these points.

After reading this Guide

✓ After reading this guide you should be able to

1. Understand Risk

- a. the main standards and how they fit together
- b. the key risk factors, especially known exploitation or likelihood of exploitation

2. Prioritize CVEs by Risk

- a. apply this understanding to Prioritize CVEs by Risk for your organization resulting in
 - i. a significant reduction in your security effort
 - ii. a significant improvement in your security posture by remediating the higher risk vulnerabilities first

3. Apply the provided guidance to your environment

- a. the source code used to do much of the analysis in this guide is provided - so you can apply it to your internal data
- b. compare what other users, and tool vendors, are doing for Risk Based Prioritization so you can compare it to what you're doing
- c. ask more informed questions of your tool/solution provider

Intended Audience

The intended audience is people in these roles:

- **Product Engineer:** the technical roles: Developer, Product Security, DevSecOps
- **Security Manager:** the non-technical business roles: includes CISO
- **Cyber Defender:** network defenders, IT/infosec
- **Tool Provider:** Tool providers: Tool Vendors, open source tools,...

This is a subset of the [Personas/Roles defined in the Requirements chapter](#).

No prior knowledge is assumed to read the guide - it provides just enough information to understand the advanced topics covered.

A basic knowledge of Jupyter Python is required to run the code (with the data provided or on your data).



Vulnerability Landscape



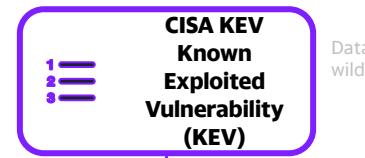
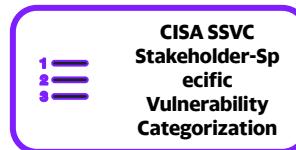
Vulnerability Landscape

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/>



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>

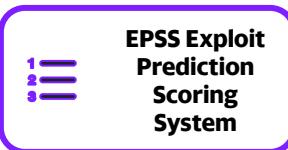


Database; source of vulnerabilities that have been exploited in the wild <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Adds enhanced information for each record such as fix information, severity scores, and impact ratings to create CVSS Score
<https://nvd.nist.gov/>

CVSS Data



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/>

Formula for scoring



Provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity <https://www.first.org/cvss/>

Alternative to?

CVE and NVD are sponsored by [U.S. Department of Homeland Security \(DHS\) Cybersecurity and Infrastructure Security Agency \(CISA\)](#)

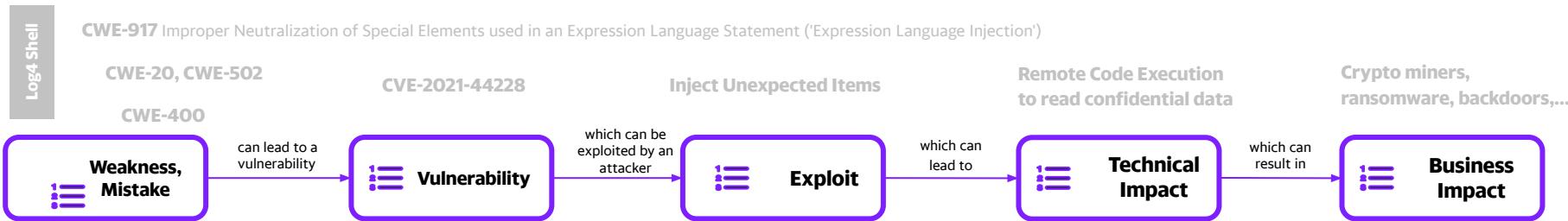
FIRST (Forum of Incident Response and Security Teams) first.org

Vulnerability

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.”



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



Vulnerability Reality

Why Should I Care?

Problem

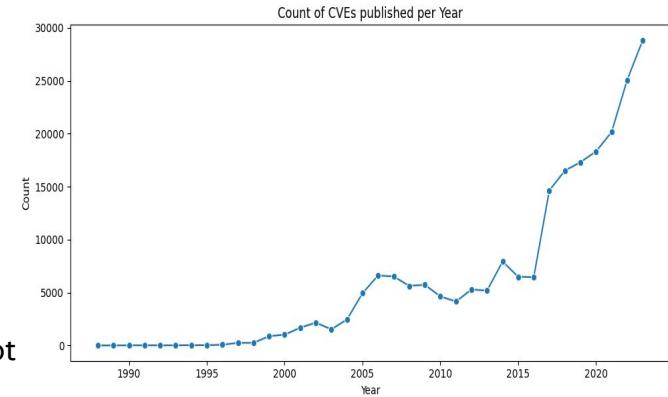
- There is an explosion in the number of published CVEs (~100/day)
- Organizations are drowning in a sea of vulnerabilities, not knowing what to remediate first

Currently

- Many organizations, and industries (PCI, FedRAMP), use CVSS Base scores alone to determine what to remediate (even though the CVSS guide says not to).

Solution

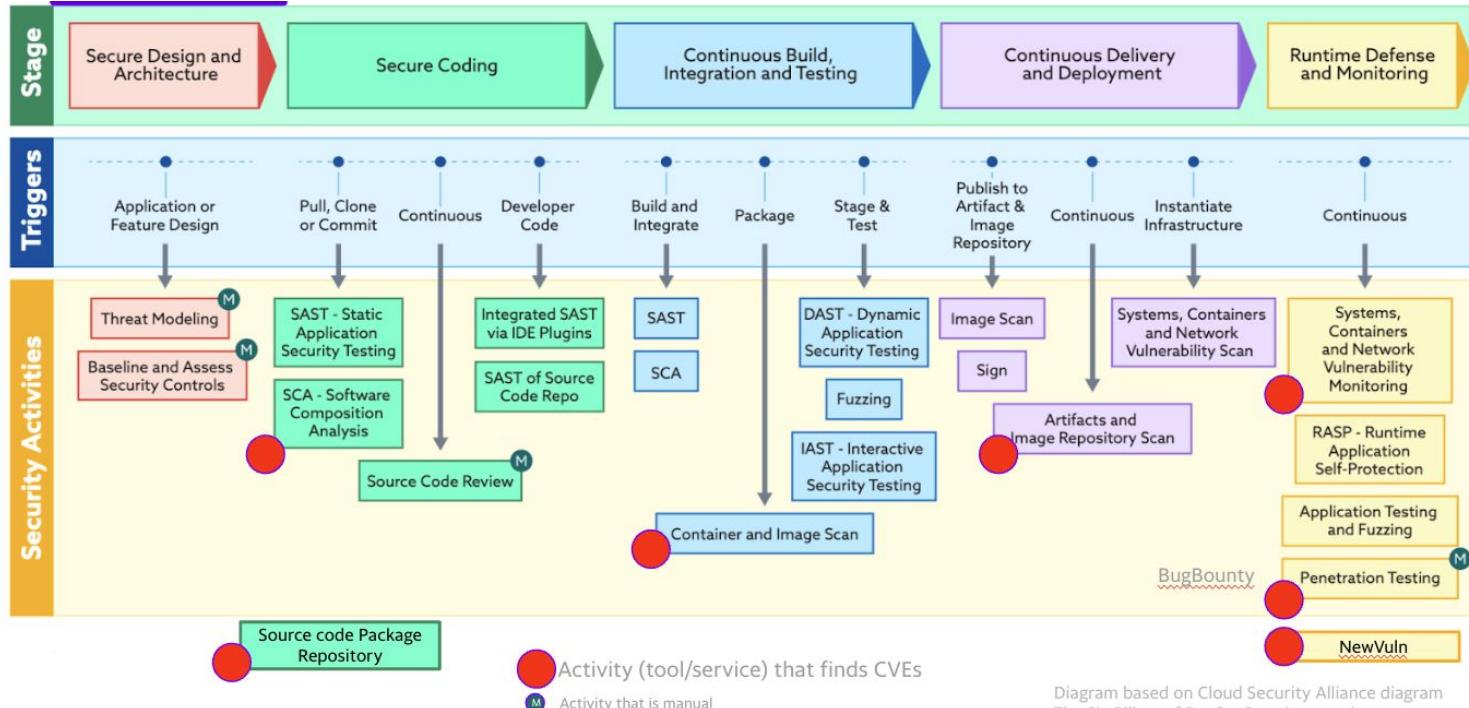
- Prioritizing vulnerabilities by **Exploitation** (as recommended by CISA, Gartner): being exploited in the wild, or are more likely to be exploited, significantly reduces the
 - cost of vulnerability management
 - risk by reducing the time adversaries have access to vulnerable systems they are trying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



The count of published CVEs is increasing at a significant rate!

Are you in?

DevOps Tools & Services that Detect CVEs



~80% of the software in products is Open Source.

Different tools/services in different stages of the DevOps pipeline detect CVEs.



Exploitation

Prioritizing by Exploitation Reduces Cost and Risk

Prioritizing by exploitation reduces cost and risk

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

Quote

- "*many vulnerabilities classified as "critical" are highly complex and have never been seen exploited in the wild - in fact, less than 4% of the total number of CVEs have been publicly exploited*" (see [BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities](#)).

Cybersecurity and Infrastructure Security Agency emphasizes prioritizing remediation of vulnerabilities that are known exploited in the wild.

- "As a top priority, focus your efforts on patching the vulnerabilities that are being exploited in the wild or have competent compensating control(s) that can. This is an effective approach to risk mitigation and prevention, yet very few organizations do this. This prioritization reduces the number of vulnerabilities to deal with. This means you can put more effort into dealing with a smaller number of vulnerabilities for the greater benefit of your organization's security posture."

Gartner

How Many Vulnerabilities are Being Exploited?

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](#)

In contrast, for [CVSS \(Base Scores\)](#):

- ~15% of CVEs are ranked Critical (9+)
- ~65% of CVEs are ranked Critical or High (7+)
- ~96% of CVEs are ranked Critical or High or Medium (4+)

Exploitation: Exploiting the Asymmetry in the Data

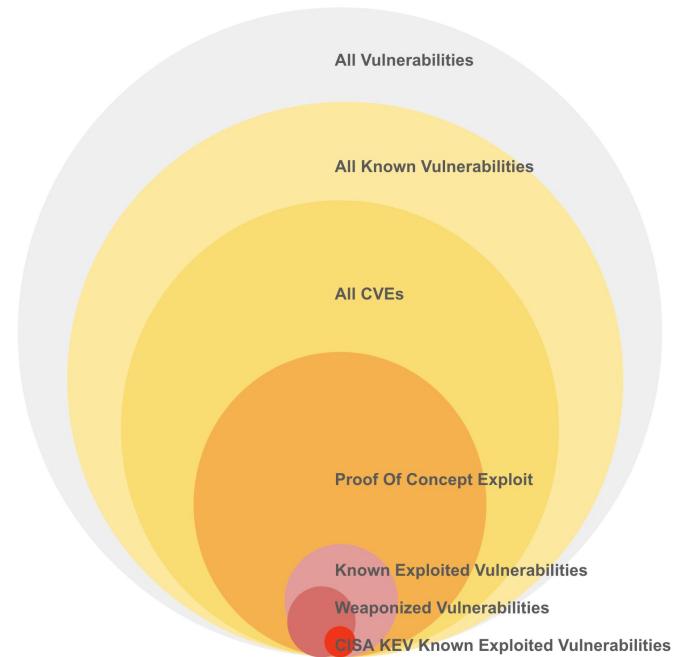
Prioritizing vulnerabilities that are being exploited in the wild, or are more likely to be exploited, reduces the

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.

~5% of CVEs are exploited, so prioritize those

How to Prioritize by Exploitation

This data can be used to determine a value for the "Exploit Maturity" in the CVSS Threat Metric Group

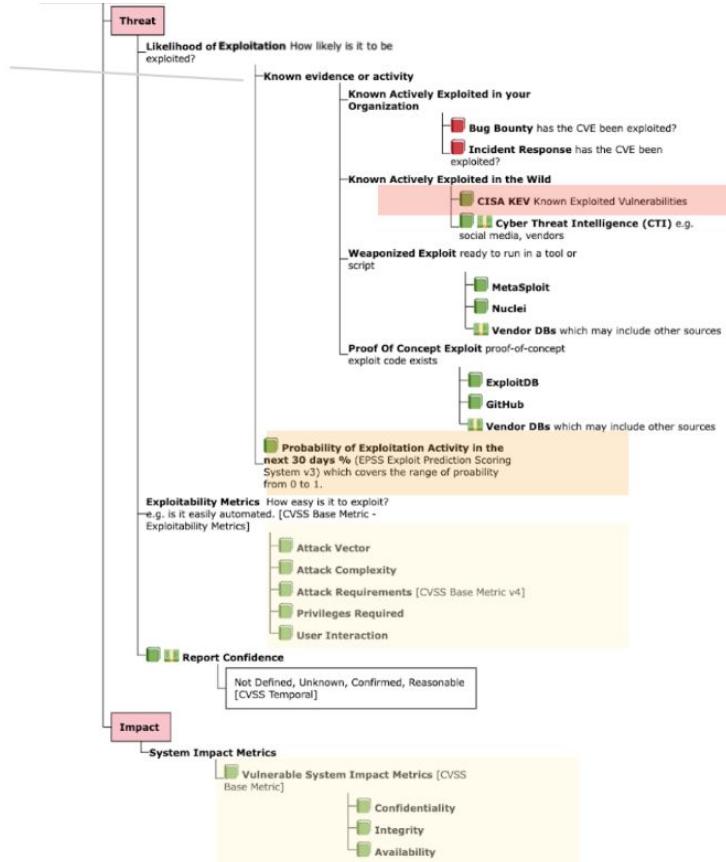
CISA KEV - Known Exploited Vulnerabilities

EPSS - Exploit Prediction Scoring System

CVSS Base Metric - Exploitability Metrics

CVSS Base Score is a combination of CVSS Exploitability and Impact Metrics

CVSS Base Metric - Impact Metrics



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

"Less than 3% of vulnerabilities have weaponized exploits or evidence of exploitation in the wild, two attributes posing the highest risk,"

"The focus should be given to those known to be exploited in the wild (CISA KEV), those with a high likelihood of exploitation (indicated by a high EPSS score), and those with weaponized exploit code available"

Exploitation

✓ Takeaways

1. There isn't a single complete authoritative source for all CVEs that are actively exploited - so we need to use multiple incomplete imperfect sources.
2. The population sizes for higher Likelihood of Exploitation (Active ~~5%, Weaponized ~~3%) are relatively small compared to Proof Of Concept (~~50%), and All CVEs (100%).
3. Not all vulnerabilities are public/known, and for those that are known, not all of them have CVEs assigned.
4. A typical enterprise will have a subset of exploits/CVEs: ~~10K order of magnitude unique CVE IDs.
 - a. The counts of these unique CVE IDs may follow a Pareto type distribution i.e. for your environment, there will likely be many instances of a small number of CVE IDs.



Exploit Prediction Scoring System (EPSS)

What is EPSS?

Exploit Prediction Scoring System (EPSS) is a data-driven effort for **estimating the likelihood (probability) that a software vulnerability will be exploited in the wild**. The Special Interest Group (SIG) consists of over 400 researchers, practitioners, government officials, and users who volunteer their time to improve this industry standard.

EPSS is managed under [FIRST](https://www.first.org/epss) (<https://www.first.org/epss>), the same international non-profit organization that manages the Common Vulnerability Scoring System (CVSS), <https://www.first.org/cvss/>.

- EPSS produces probability scores for **all known published CVEs** based on current exploitation ability, and updates these scores daily
- The scores are **free** for anyone to use
- EPSS should be used:
 - as a measure of the **threat** aspect of risk
 - when there is no other evidence of current exploitation
 - together with other measures of risk

What Does EPSS Provide?

1. EPSS Score

- a. Probability scores for all known CVEs. Specifically, the probability that each vulnerability will be exploited in the next 30 days.

b. Percentile

- i. The percentile scores represent a rank ordered list **of all CVEs** from most likely to be exploited, to least likely to be exploited

2. Coverage, Efficiency, Effort figure showing the tradeoffs between alternative remediation strategies.

- a. Specifically, this figure illustrates the tradeoffs between three key parameters that you may use when determining your optimal remediation strategy: coverage, efficiency, and level of effort

<https://api.first.org/data/v1/epss?cve=CVE-2021-44228>

```
{"cve": "CVE-2021-44228", "epss": "0.975600000", "percentile": "0.999980000", "date": "2024-05-11"}
```

EPSS V3

Improved Precision

EPSS V3 launched Mar 2023, offers improved precision at identifying vulnerabilities likely to be exploited in the wild.

- Expand the sources of exploit data by partnering with multiple organizations willing to share data for model development, and engineer more complex and informative features.
- Allowed the proposed v3 model to achieve **an overall 82% improvement in classifier performance over v2**
- This boost in prediction performance allows organizations to substantially improve their prioritization practices and design data-driven patching strategies.

Data Sources Used to Feed the EPSS V3 Model

Description	# of variables	Sources
Exploitation activity in the wild (ground truth)	1 (with dates)	Fortinet, AlienVault, ShadowServer, GreyNoise
Publicly available exploit code	3	Exploit-DB, GitHub, MetaSploit
CVE is listed/discussed on a list or website ("site")	3	CISA KEV, Google Project Zero, Trend Micro's Zero Day Initiative (ZDI)
Social media	3	Mentions/discussion on Twitter
Offensive security tools and scanners	4	Intrigue, sn1per, jaeles, nuclei
References with labels	17	MITRE CVE List, NVD
Keyword description of the vulnerability	147	Text description in MITRE CVE List
CVSS metrics	15	National Vulnerability Database (NVD)
CWE	188	National Vulnerability Database (NVD)
Vendor labels	1,096	National Vulnerability Database (NVD)
Age of the vulnerability	1	Days since CVE published in MITRE CVE list

"The exploit data used in this research paper covers activity from July 1, 2016 to December 31st, 2022 (2,374 days / 78 months / 6.5 years), over which we collected 6.4 million exploitation observations (date and CVE combinations), targeting 12,243 unique vulnerabilities. Based on this data, we find that 6.4% (12,243 of 192,035) of all published vulnerabilities were observed to be exploited during this period"

► EPSS v3 allows organizations to substantially improve their prioritization practices

Tools/Vendors using EPSS

Vendor	Product
AppSoc	Risk-Based Application Security Posture Management
Aqua Security	Aqua Workload Protection
Armis	Armis Asset Vulnerability Management module
Armo Security	Armo Kubernetes Security
Armorcode	Risk-Based Vulnerability Management
Avalor	Avalor Security Data Fabric
AWS	Inspector
Axonius	Vulnerability Management Module
Backlash	Reachability SAST/SCA
Binary	Transparency Platform
Bomber	Bomber
Brinqa	Cyber Risk Platform
Boost Security	DevSecOps Platform
Cavelo	Attack Surface Management
cvefeed.io	Vulnerability Intelligence
Cisco	Kenna Security

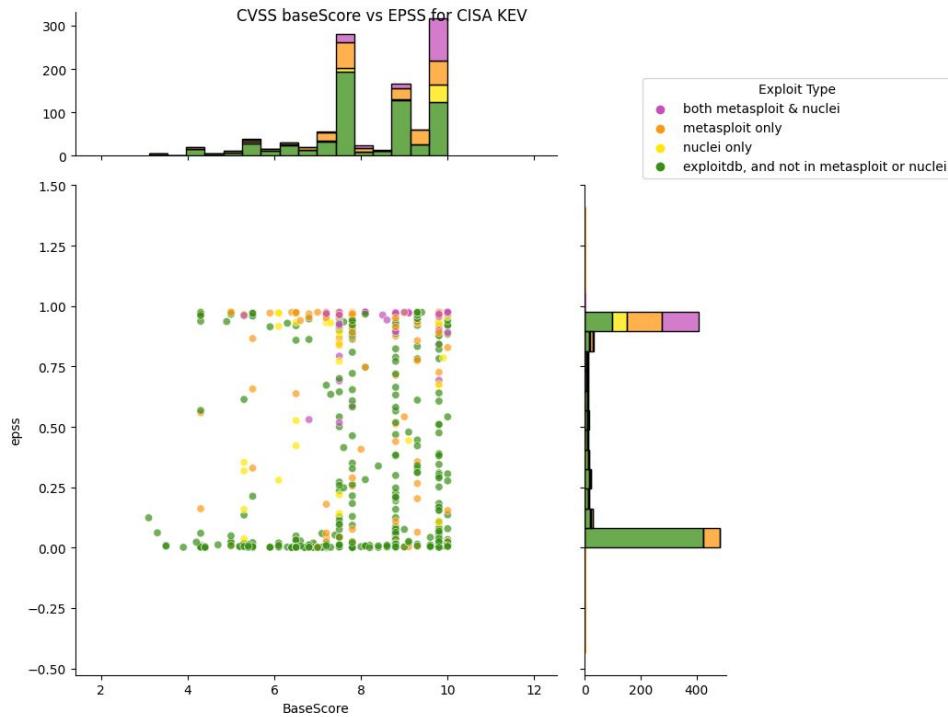
>100 Tools/Vendors are using EPSS - including some of the best known.



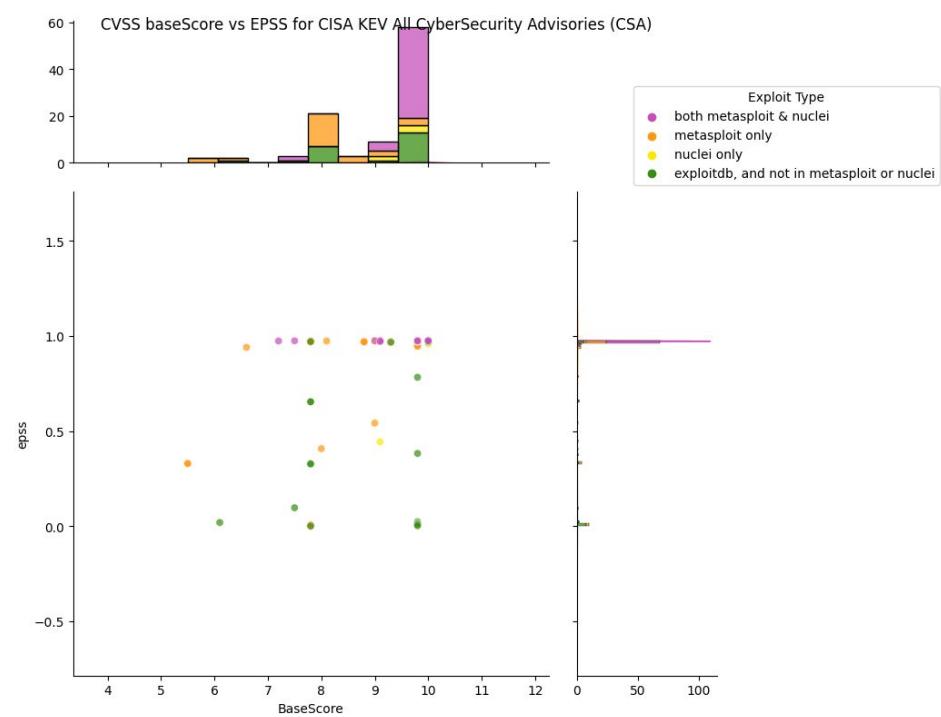
EPSS Applied

CISA Known Exploited Vulnerabilities (CISA KEV)

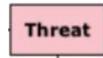
CISA KEV



CyberSecurity Advisories (CSA)



Exploitation Data Sources with EPSS



Likelihood of Exploitation How likely is it to be exploited?

Known Evidence or Activity

Known Actively Exploited in your Organization

- Bug Bounty has the CVE been exploited?
- Incident Response has the CVE been exploited?

Known Actively Exploited in the Wild

- CISA KEV Known Exploited Vulnerabilities
- Cyber Threat Intelligence (CTI) e.g. social media, vendors

Weaponized Exploit

 ready to run in a tool or script

- MetaSploit
- Nuclei

- Vendor DBs which may include other sources

Proof Of Concept Exploit

 proof-of-concept exploit code exists

- ExploitDB
- Github

- Vendor DBs which may include other sources

Probability of Exploitation Activity in the next 30 days % (EPSS Exploit Prediction Scoring System v3) which covers the range of probability from 0 to 1.

For the ~5% of CVEs with known evidence of exploitation, or high EPSS scores:

	EPSS HIGH	EPSS LOW
Active Exploitation		
No Known Evidence		
Prioritize First	Prioritize First	Prioritize Next

EPSS for YOUR Environment

 If YOUR environment is similar to the EPSS model environment, then a similar probability of exploitation activity should apply to YOUR environment, and therefore the EPSS scores for the CVEs in your environment.

” Quote

Organizations should measure and validate the usefulness of EPSS in their environments. No organization should assume that its environment matches the data used to train EPSS. However, many organizations' environments should be a near-enough match.

[Probably Don't Rely on EPSS Yet](#), Jonathan Spring, June 6, 2022

 EPSS is best suited to enterprise environments

” Quote

Similarly, these detection systems will be typically installed on public-facing perimeter internet devices, and therefore less suited to detecting computer attacks against internet of things (IoT) devices, automotive networks, ICS, SCADA, operational technology (OT), medical devices, etc

[Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights](#), Feb 2023

EPSS is best suited to network based attacks

EPSS is best suited to network based attacks

Vulnerabilities that are remotely exploitable (i.e. Network Attack Vector in CVSS Base Score terms) have a higher Exploitability (CVSS Base Score Exploitability metrics group)

1. remotely exploitable versus those that require physical or local proximity.
2. can be exercised automatically over the network without requiring user-interaction (e.g. clicking a button or a link).

EPSS is best suited to these types of vulnerabilities.

Quote

Moreover, the nature of the detection devices generating the events will be biased toward detecting network based attacks, as opposed to attacks from other attack vectors such as host-based attacks or methods requiring physical proximity

[Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights, Feb 2023](#)

Example

At the time of writing this guide, [CISA Warns of Active Exploitation Apple iOS and macOS Vulnerability](#).

This CVE has a consistently low EPSS score near zero (<https://api.first.org/data/v1/epss?cve=CVE-2022-48618&scope=time-series>).

This is to be expected because the CVE Attack Vector is "Local", not Network, per (<https://nvd.nist.gov/vuln/detail/CVE-2022-48618>)

Zero Days

” Quote

EPSS scores won't be available for Zero Days (because EPSS depends on the CVE being published and it can take several days for the associated CVE to be published).

"The State of Exploit Development: 80% of Exploits Publish Faster than CVEs".

” Quote

Zero day vulnerabilities made up only approximately 0.4% of vulnerabilities during the past decade. The amount spent on trying to detect them is out of kilter with the actual risks they pose. This is compared with the massive numbers of breaches and infections that come from a small number of known vulnerabilities that are being repeatedly exploited. As a top priority, focus your efforts on patching the vulnerabilities that are being exploited in the wild or have competent compensating control(s) that can. This is an effective approach to risk mitigation and prevention, yet very few organizations do this.

Focus on the Biggest Security Threats, Not the Most Publicized, Gartner, Nov 2017

Takeaways

✓ Takeaways

1. CVSS or EPSS should not be used alone to assess risk - they can be used together:
 - a. CVSS Base Score is a combination of Exploitability and Impact
 - b. Various data sources can be used as evidence of exploitation activity or likelihood of exploitation activity - but there isn't
 - i. a single authoritative source
 - ii. an industry standard on how to do this
2. EPSS should be used with other exploitation evidence; if there is an absence of exploitation evidence, then EPSS can be used to estimate the probability it will be exploited.
3. EPSS scores won't be available for Zero-Days
4. "Don't go chasing zero days, patch your known vulnerabilities instead"
5. It is the responsibility of the CVSS Consumer/user to populate the CVSS Exploit Maturity values i.e. unlike the CVSS Base Score, these are not provided.
6. Criteria for "Exploitation" are different for EPSS and CISA KEV.



EPSS Thresholds

User Request: EPSS Security Levels

Related User Scenarios and User Stories

Fit EPSS to CVSS Ratings

Quote

This is put into easy-to-understand severity levels that additionally factor in the confidence of the likelihood score and are aligned with the existing Critical, High, Medium, Low severities I am used to from CVSS.

Severity Categories

Quote

As a Tool Provider I want to provide my customers with not just an EPSS Score, but a standard Severity level that is familiar to me and officially provided by the same organization that provides the scores. Critical, High, Medium, Low are values I understand and can be mapped to existing policies and processes easily - especially for communication to less security-fluent stakeholders.

Feedback

CVSS already includes support for Exploitation in CVSS Exploit Maturity.

- See section CVSS Exploit Maturity for more details, including
 - the limitations of using CVSS Exploit Maturity for risk-based prioritization
 - an example project that calculates CVSS Exploit Maturity and includes EPSS scores and thresholds

User Request: EPSS As the Single Score for Exploitation

EPSS as the Single Score for Exploitation

Quote

"Ideally, EPSS scores would factor in already published exploits"

Existing Public Exploits

A similar common request is to

Quote

"set the EPSS score to 1 if there are already published exploits"

Feedback

Per [Using EPSS with Known Exploitation](#), EPSS is pre-threat intel and should be used in conjunction with evidence that a vulnerability is being exploited. **EPSS is by design not "the Single Score for Exploitation"**

See <https://www.first.org/epss/faq#Everyone-knows-this-vulnerability-has-been-exploited-why-doesn-t-EPSS-score-it-at-100>

Per [CVSS](#):

Quote

it is recommended to use multiple sources of threat intelligence as many are not comprehensive.

EPSS V3

Precision (efficiency) measures how well resources are being allocated, (where low efficiency represents wasted effort), and

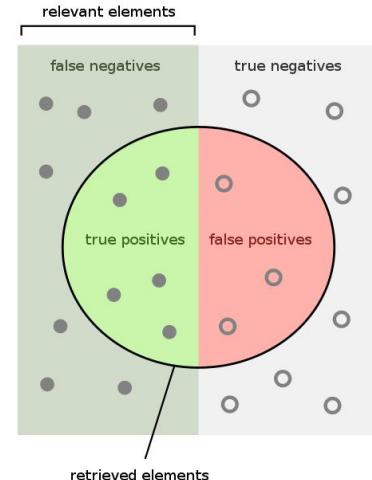
- calculated as the **true positives divided by the sum of the true and false positives.**
- In the vulnerability management context, efficiency addresses the question, “out of all the vulnerabilities remediated, how many were actually exploited?”
- If a remediation strategy suggests patching 100 vulnerabilities, 60 of which were exploited, the efficiency would be 60%.

Recall (coverage), on the other hand, considers how well a remediation strategy actually addresses those vulnerabilities that should be patched (e.g., that have observed exploitation activity),

- calculated as the **true positives divided by the sum of the true positives and false negatives.**
- In the vulnerability management context, coverage addresses the question, “out of all the vulnerabilities that are being exploited, how many were actually remediated?”
- If 100 vulnerabilities are exploited, 40 of which are patched, the coverage would be 40%.

Precision: how many retrieved items are relevant?

Recall: how many relevant items are retrieved?



$$\text{Precision} = \frac{\text{true positives}}{\text{true positives} + \text{false positives}}$$
$$\text{Recall} = \frac{\text{true positives}}{\text{true positives} + \text{false negatives}}$$

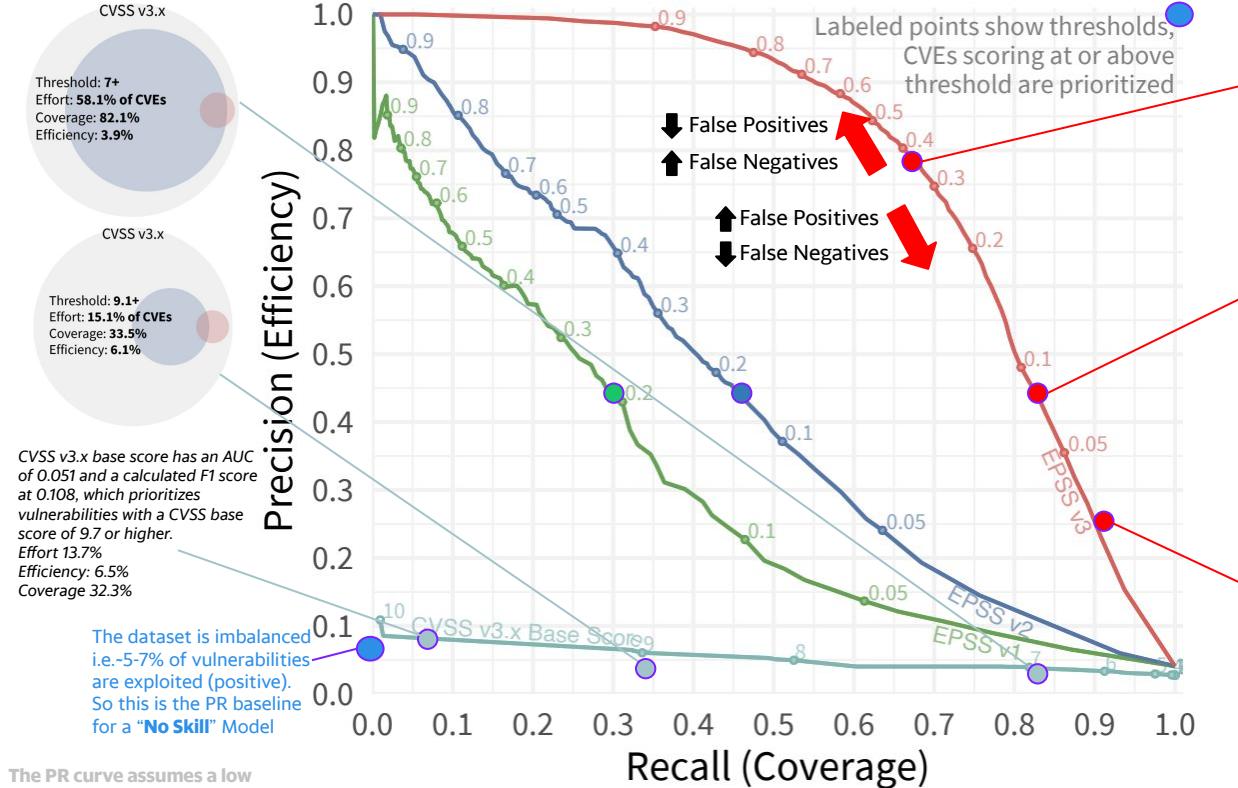
https://en.wikipedia.org/wiki/Precision_and_recall

“Relevant elements” is Exploited CVEs in our case.

A PR curve is drawn by picking Threshold values, then working out the PR values.

What EPSS Threshold to use?

Perfect skill



V3: Area under the curve (AUC) of 0.7795

Remediation strategy based on the F1 score of 0.728
 F1 assumes False Positives/Precision and False Negatives/Recall are equally Important. $F1 = 2TP/(2TP+FP+FN)$

Threshold: 0.36+
 Effort: This strategy would prioritize remediation of 3.5% of CVEs
 Efficiency: 78.5%
 Coverage: 67.8%

"If it's got a high EPSS score I should definitely be worried about it.
 If it's got a low EPSS score, I can't be certain whether I should be worried or not.

So we need to pick an EPSS threshold high enough that it is telling me something, but low enough that I don't miss CVEs that I should be fixing."

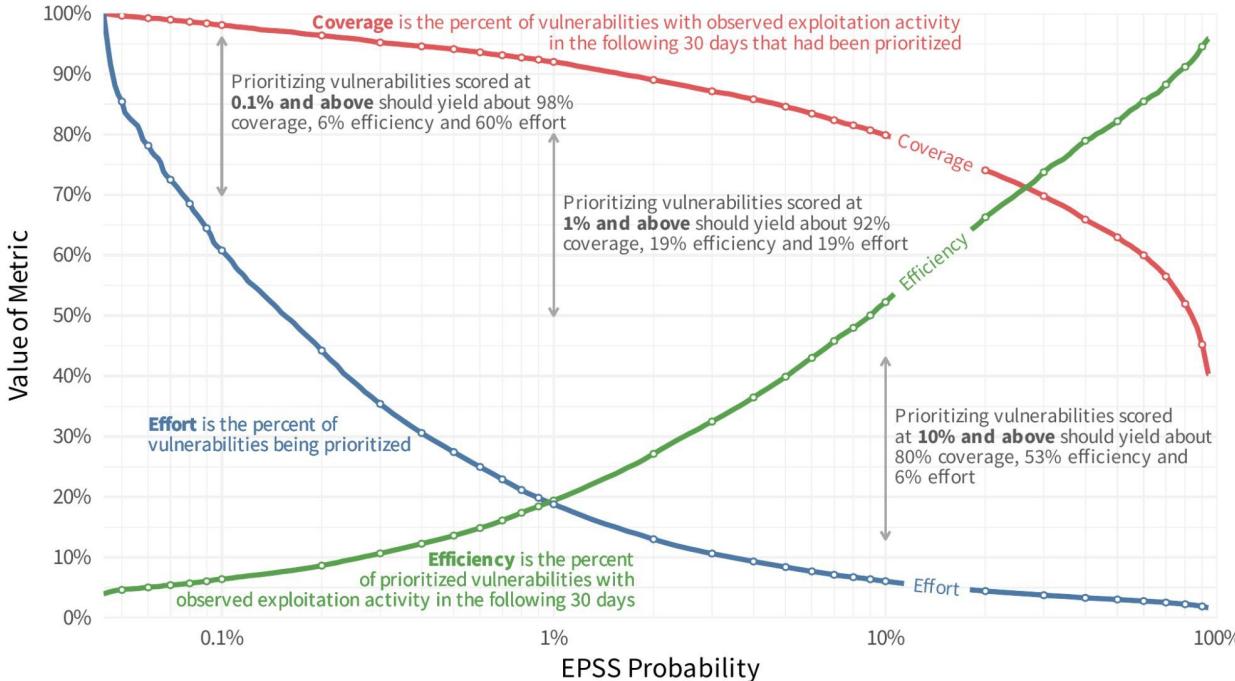


Pick EPSS Threshold per above. Start Conservative. Adjust based on YOUR CVE data.

What EPSS Threshold do I use?

Picking Thresholds for EPSS

Select a threshold for EPSS along the horizontal and trace it to each metric to determine the coverage, efficiency and level of effort. This represents the performance of EPSS from March 7 to November 1, 2023.

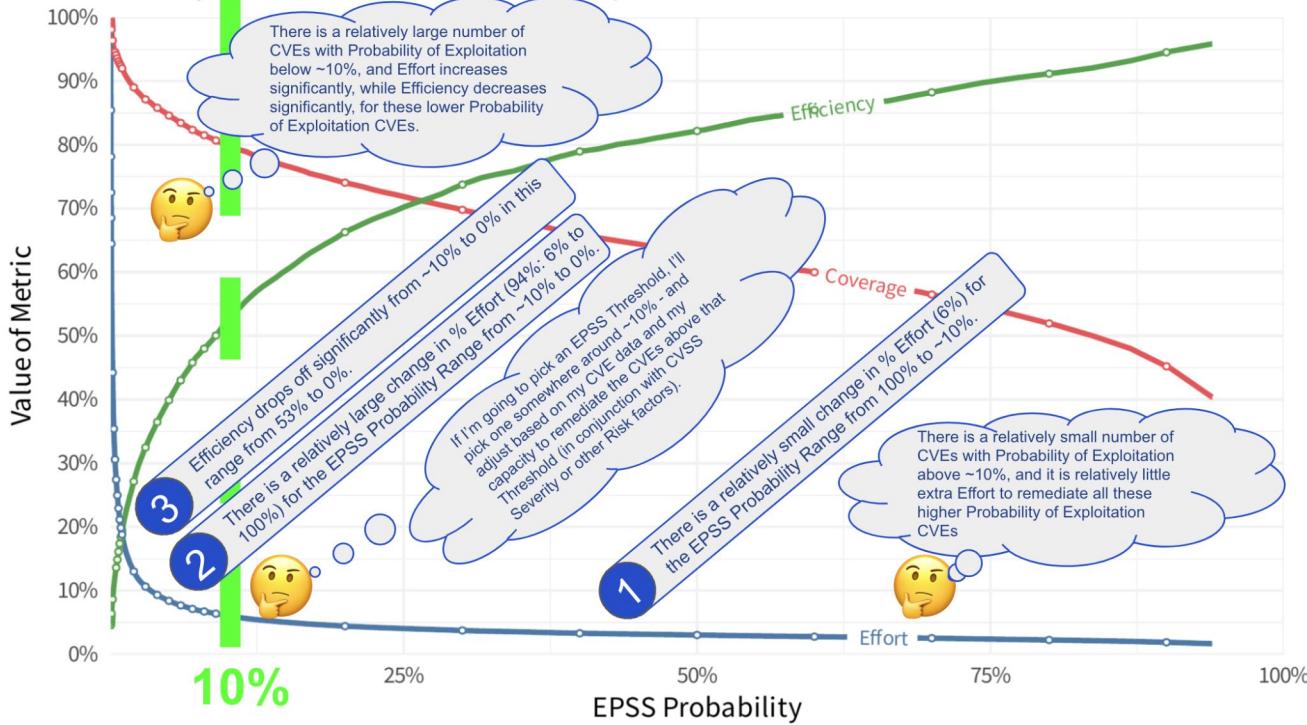


Source: <https://first.org/epss>

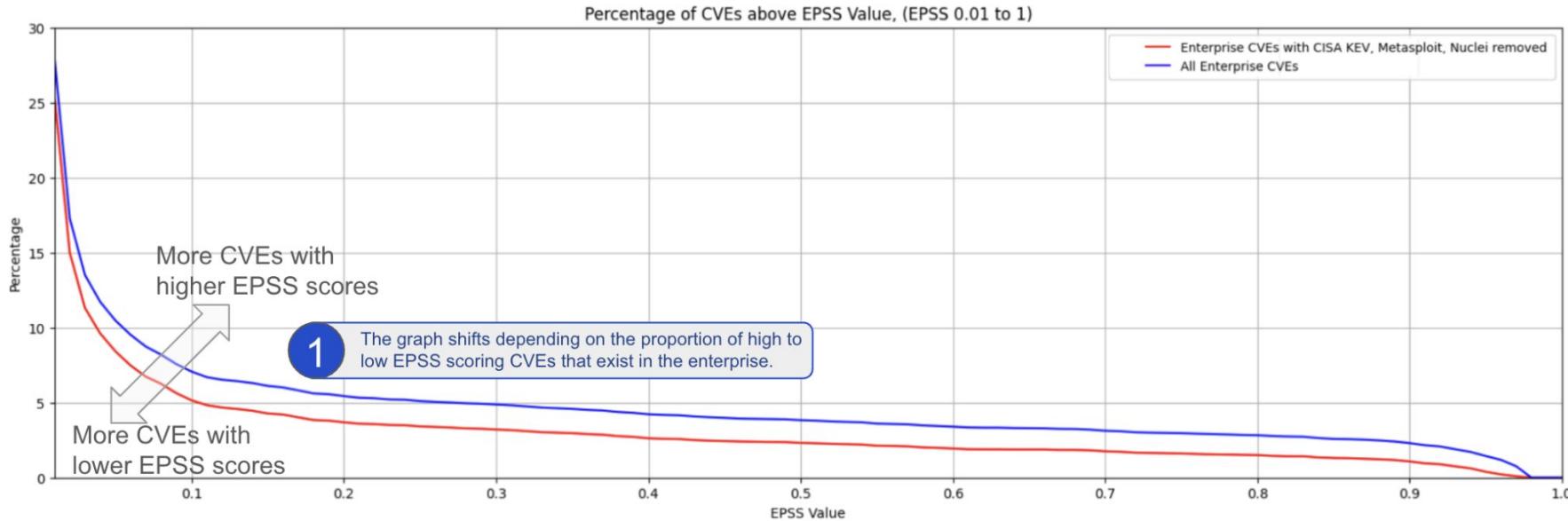
What EPSS Threshold do I use?

Picking Thresholds for EPSS

Select a threshold for EPSS along the horizontal and trace it to each metric to determine the coverage, efficiency and level of effort. This represents the performance of EPSS from March 7 to November 1, 2023.



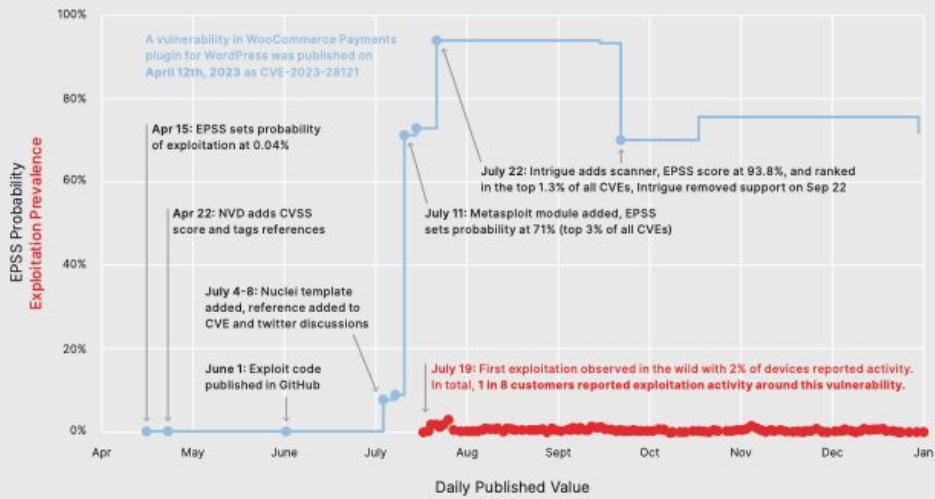
EPSS



Here we use EdgeScan detected CVEs as the representative data set for our Enterprise.

EPSS Dynamic Signal - Fortinet 2H 2023 Report

Evolution of EPSS and the exploitation of the WooCommerce vulnerability



CVE2023-28121: This CVE was published on April 12, 2023, and was initially assessed by EPSS as having a low probability of exploitation. That assessment was revised dramatically after a Nuclei template and Metasploit module were released in early July. Given these changes, the vulnerability rose to the top 3% of EPSS scores with a 71% chance of exploitation in the next 30 days.

Shortly after this revision of EPSS, our team observed the first signs of exploitation in the wild on July 19. In this case, **EPSS provided an effective early warning system prior to the outbreak of attacks, giving defenders a valuable head start on remediation.**

In each threat landscape report, we aim to determine how long it takes for a vulnerability to move from initial release to exploitation and whether vulnerabilities with a high Exploit Prediction Scoring System (EPSS) score are exploited faster.

For the new exploits identified, attacks occurred an average of 4.76 days after discovery, which is 43% faster than the time-to-exploitation observed in 1H 2023. This underscores the need to use EPSS as an early warning system, as well as the importance of prioritizing patching efforts to mitigate the vulnerabilities most likely to be exploited.



Risk Based Prioritization

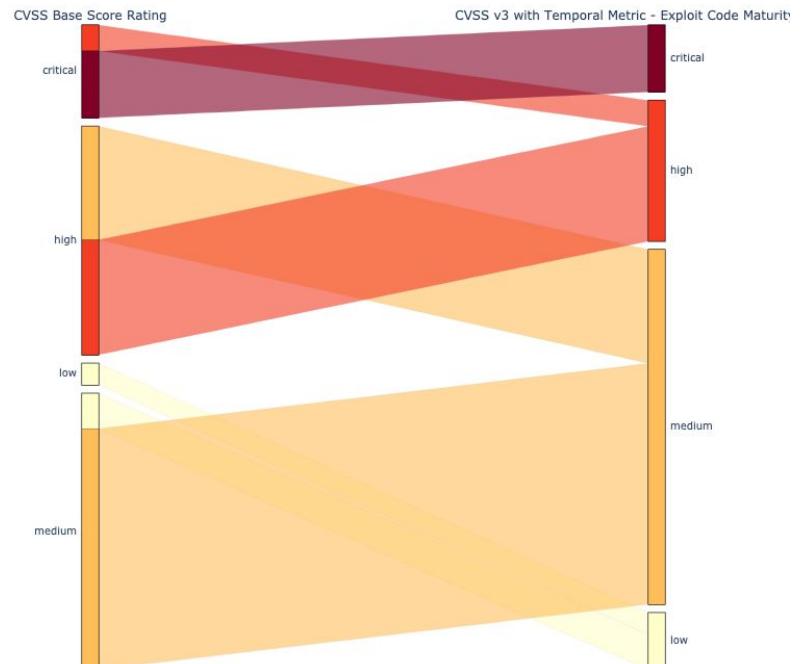
So What? For Exploitation Evidence and EPSS. CVSS

The CVSS Standard supports Exploitation Evidence as an input: Temporal – Exploit Code Maturity (E).
CISA KEV, EPSS can be used as inputs here.

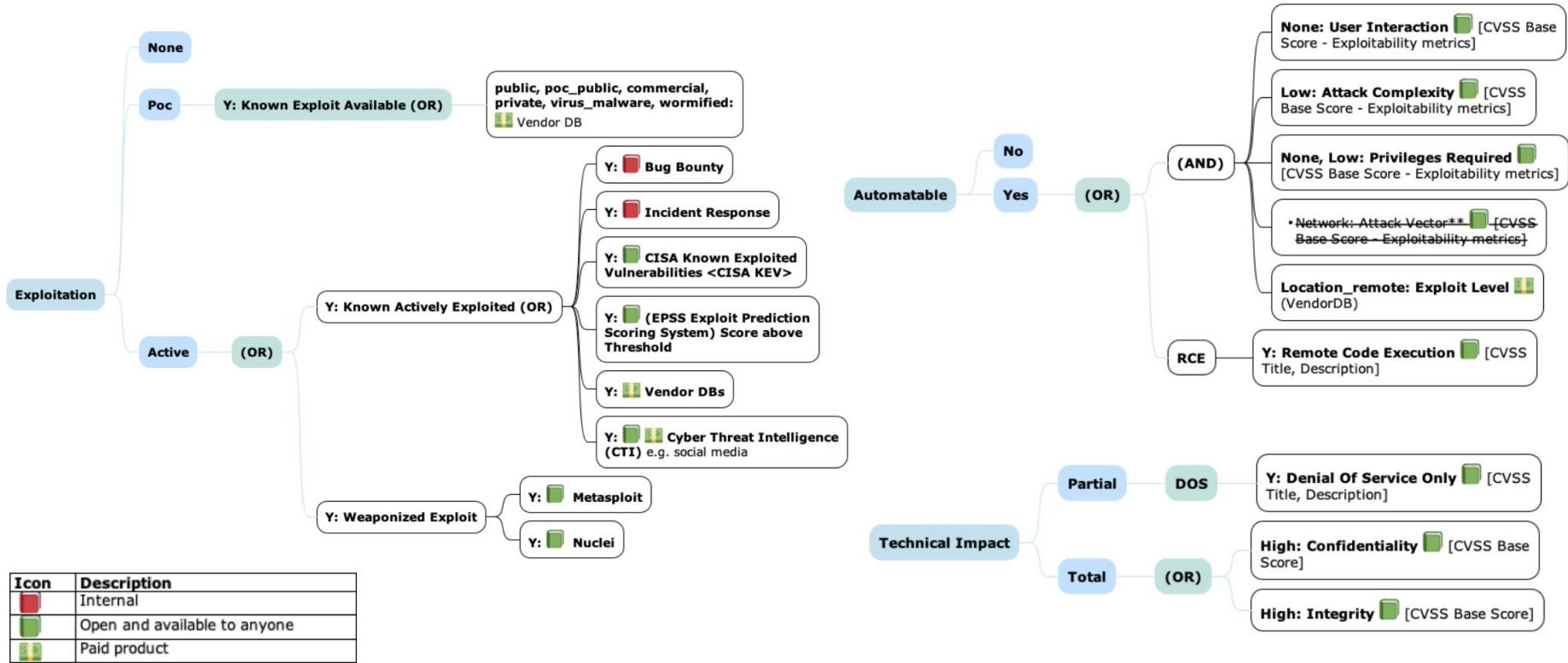
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Temporal Score, i.e., it has the same effect on scoring as assigning High.
High (H)	Functional autonomous code exists, or no exploit is required (manual trigger) and details are widely available. Exploit code works in every situation, or is actively being delivered via an autonomous agent (such as a worm or virus). Network-connected systems are likely to encounter scanning or exploitation attempts. Exploit development has reached the level of reliable, widely available, easy-to-use automated tools.
Functional (F)	Functional exploit code is available. The code works in most situations where the vulnerability exists.
Proof-of-Concept (P)	Proof-of-concept exploit code is available, or an attack demonstration is not practical for most systems. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.
Unproven (U)	No exploit code is available, or an exploit is theoretical.

This has the effect of reducing CVSS scores – though not significantly.
Other more-effective schemes are discussed in the guide.

CVSS-B Base vs CVSS v3 with Temporal Metric - Exploit Code Maturity (E) Score

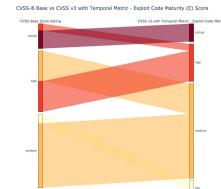
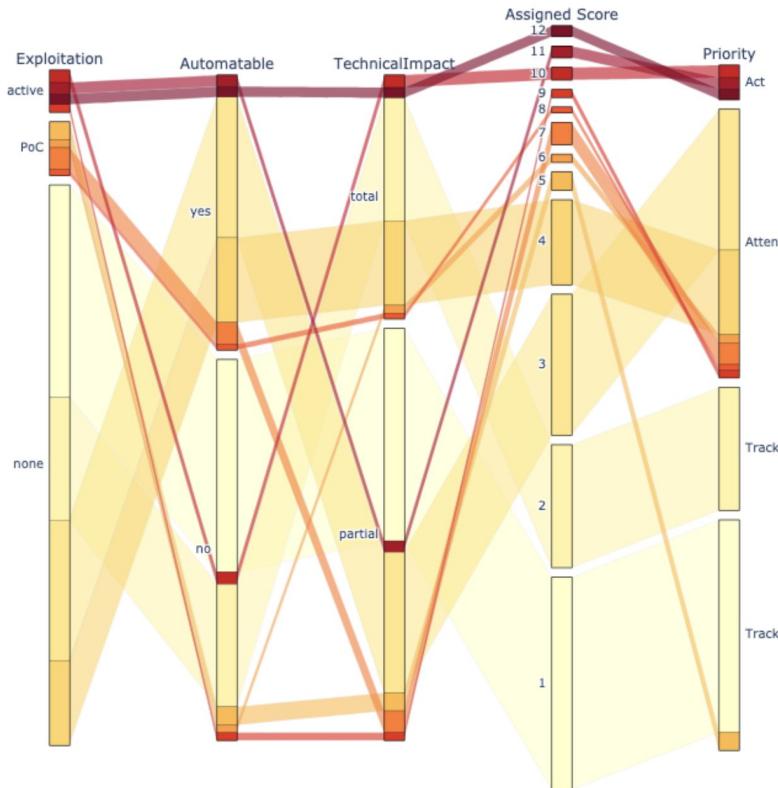
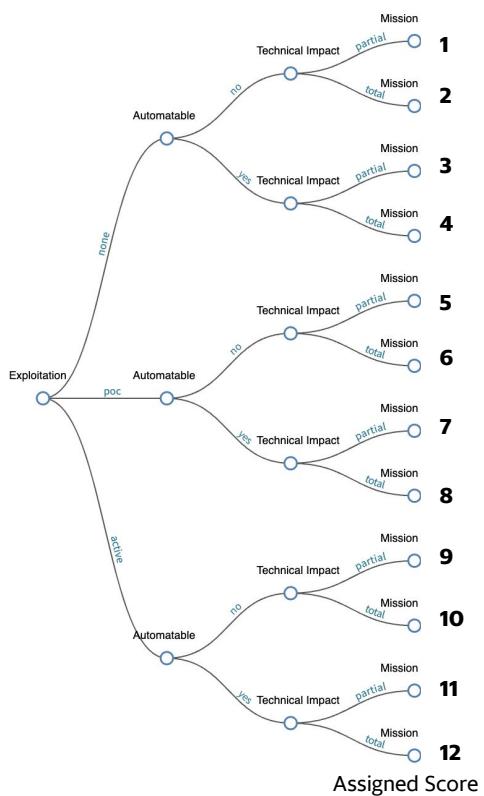


Risk-based Decision Tree Decision Node Inputs



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

So What? For Exploitation Evidence and EPSS. SSVC



CVSS

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



Roadmap

EPSS Dynamic Signal

Time variance of an EPSS score for a CVE #6

Open



RiskBasedPrioritization/RiskBasedPrioritization.github.io

Public



Crashedmind opened on Feb 15

edited by Crashedmind · Edits · ...

Description, Use Case and User Stories

There is signal in the temporal/dynamic aspects of EPSS (in addition to the threshold approach as outlined in the guide.)

So we want to provide a user-centric guide on how to use this signal - and the associated use cases e.g. what's fast incoming? e.g. threat hunting, threat intelligence,...

Definition of Ready

1. The people who will lead this effort are identified and interested and committed.
2. There's a rough plan agreed.

Acceptance Criteria

1. User scenarios are defined for this EPSS signal
2. Users who represent the user scenarios are identified and provide user feedback on the chapter
3. The chapter will be presented at the EPSS SIG for socialization and feedback.

Additional context

Several articles have been published e.g.

1. <https://www.linkedin.com/pulse/day-life-epss-bonus-rudy-guyonneau-phd-dvzge/>
2. https://www.linkedin.com/posts/parisel_security-soc-cert-activity-7175484806946811905-WJIS



EPSS Dynamic Signal

Time variance of an EPSS score for a CVE #6

Rudy Guyonneau - OryxLabs

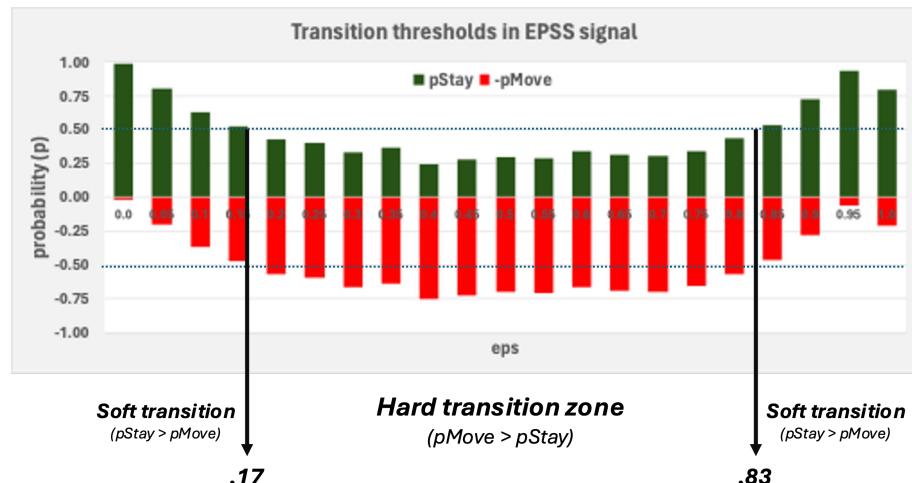
Christophe Parisel

Proactivity in CVE Remediation based on early EPSS signal

Can eps data upon onset predict eps at later stages ?

WIP. Evidence of eps-dependent transitioning

i.e. “upon change, a CVE’s EPSS score is more likely to move outside of its bracket than not between .17 and .83”



EPSS v3, data from April 1st, 2023 to November 30th, 2023

Aggregate Probability of Exploitation

Guidance on how to combine EPSS scores #7

  RiskBasedPrioritization/RiskBasedPrioritization.github.io  Public

Crashedmind opened on Feb 15 ...

Description, Use Case and User Stories
Guidance on how to combine EPSS Probability scores for a group of related CVEs with associated EPSS scores.
See thread <https://epss-wg.slack.com/archives/C01351T3L9W/p1697053753184899>

Definition of Ready
(Assignee lists the things they need from the Requestor to be able to start work on this)

Acceptance Criteria
(Requestor lists the things they need the deliverable to be able to accept this from the Assignee)

Additional context

Example
Should there be some grouping going on for these types of scenarios when it's not a 1:1? Like sum up and divide by the count of CVE's or default to the highest EPSS score of the group, or...?

Vuln Title: Google Chrome Prior to 115.0.5790.170 Multiple Vulnerabilities
Severity: 4
CVSS 3.1 Base: 8.8
Associated CVE's: [GHSA-9xxv-mx64-rx27](#)
So if I break those CVE's out I get this:
CVE.ID CVSS 3.1 Base EPSS Score EPSS Percentage
[GHSA-wh89-h5f7-hhcr](#) 8.1 0.00084 0.34929
[GHSA-g63v-hwv9-j9q5](#) 8.8 0.00082 0.34015
[GHSA-9xxv-mx64-rx27](#) 8.1 0.00084 0.34929
[GHSA-qc3g-vp59-7vwh](#) 8.8 0.00082 0.34015
[GHSA-9j4r-qr47-rcxp](#) 8.8 0.00085 0.3532

consider an organization with 100 vulnerabilities, each with a 5% chance of being exploited. The question of great interest to a network defender might be: what is the probability that at least one of those vulnerabilities will be exploited, and therefore what is my overall threat?

The probability of no vulnerabilities is the linear product of each vulnerability not being exploited



How did that happen?



Vulnerability Landscape



Vulnerability Reality



Exploitation



Exploit Prediction Scoring System (EPSS)



EPSS Applied



EPSS Thresholds



Risk Based Prioritization



Roadmap

Recap



Takeaways

✓ Takeaways

Prioritize vulnerabilities by Exploitation to Reduce Cost and Risk

Only about 5% or fewer of all [CVEs have been exploited](#).

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

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

Use a [Risk Based Prioritization Scheme](#) that supports Exploitation Evidence and Likelihood Of Exploitation (EPSS)

"The focus should be given to those known to be [exploited in the wild \(CISA KEV\)](#), those with a high likelihood of exploitation (indicated by a high [EPSS score](#)), and those with weaponized exploit code available"

Refine the [Risk Based Prioritization scheme](#) based on your environment and your data.

1. Use CVEs detected in your Incident Response, Bug Bounty, PenTesting findings to inform your [Risk](#).
2. For EPSS:
 - a. Assess [EPSS for YOUR Environment](#)
 - b. Start by picking an [EPSS Threshold](#) around 10%, and adjust based on your [CVE data](#) and your capacity to [remediate the CVEs above that Threshold](#) (in conjunction with [CVSS Severity](#) or other [Risk factors](#)) per [Remediation Policy for an Enterprise](#)

THANK YOU!



- ★ Jay Jacobs (EPSS creator and EPSS SIG co-chair)
 - ★ Contributors to the guide
 - ★ **Yahoo** for cultivating such a rich environment for people to thrive, and putting People first
 - ★ **BSidesDub** Anthi Gilligan, Dave Harbourne, Dylan, Nadine and all the crew
-
- ★ **You** for sharing 40 minutes of your lives with me.

The End



<https://riskbasedprioritization.github.io/>



0 (8)



How did that happen?
5 (6)



Vulnerability Landscape
8 (2)



Vulnerability Reality
10 (2)



Exploitation
13 (5)



Exploit Prediction Scoring
System (EPSS)
18 (4)



EPSS Applied
22 (5)



Risk Based Prioritization
32 (3)



Roadmap
36 (3)

Timing

