Hitchhiker's Guide to the Vulniverse

DON'T PANIC

Here's how all this stuff works!

Who is this clown?

CRob

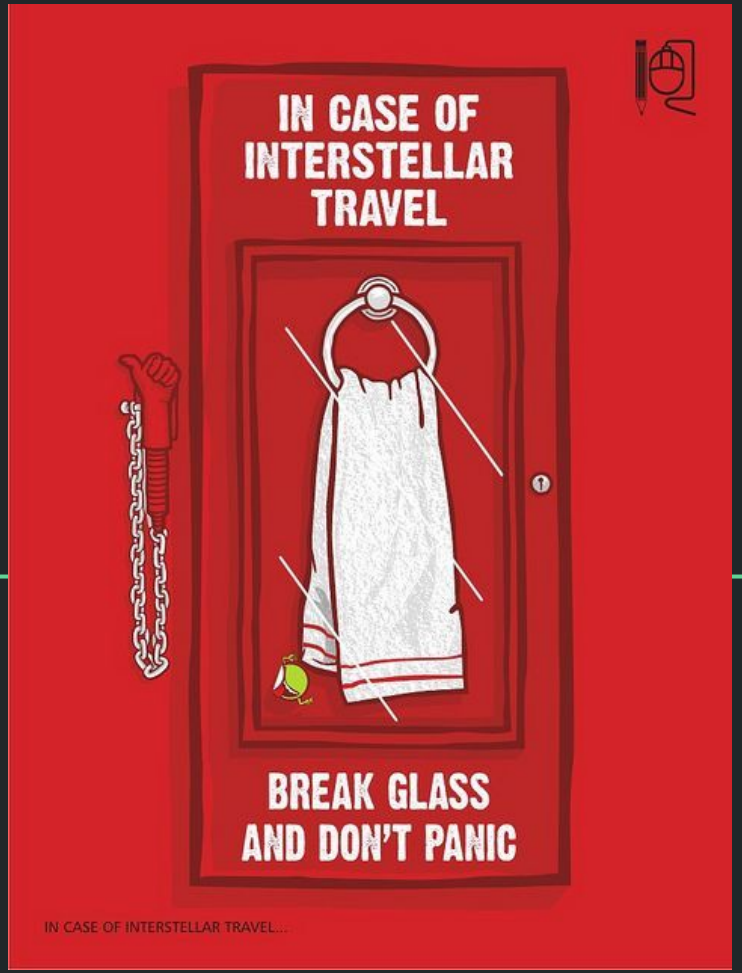
Cat Herder, Security Lorax


DON'T
PANIC

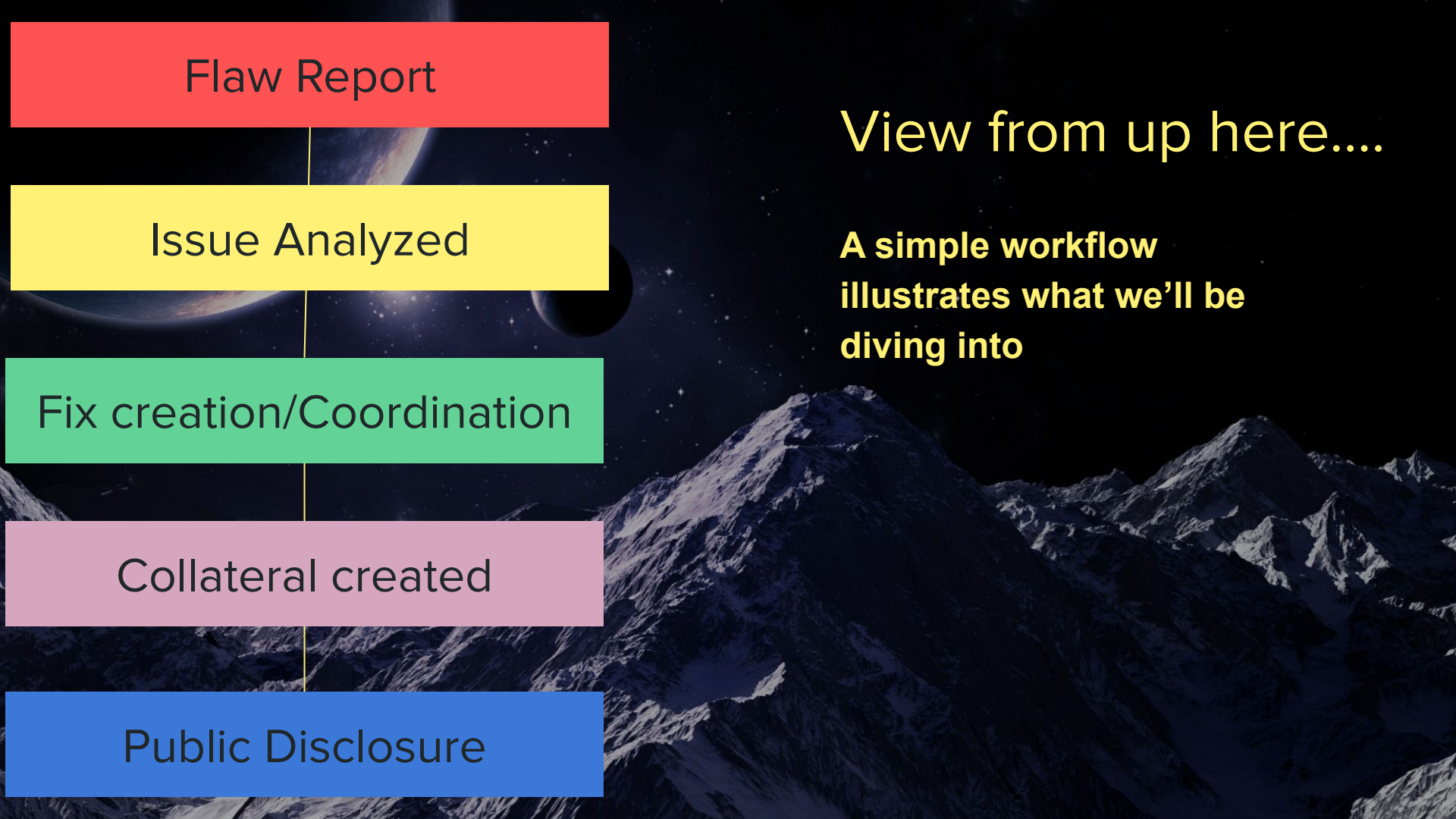
Why Are We Here?

- The practice of “The Security” can be complex and jargon-filled.
- There are many critical aspects that have similar-sounding names/acronyms.
- **Computers are hard.**

So grab a towel and put your sunglasses on.....

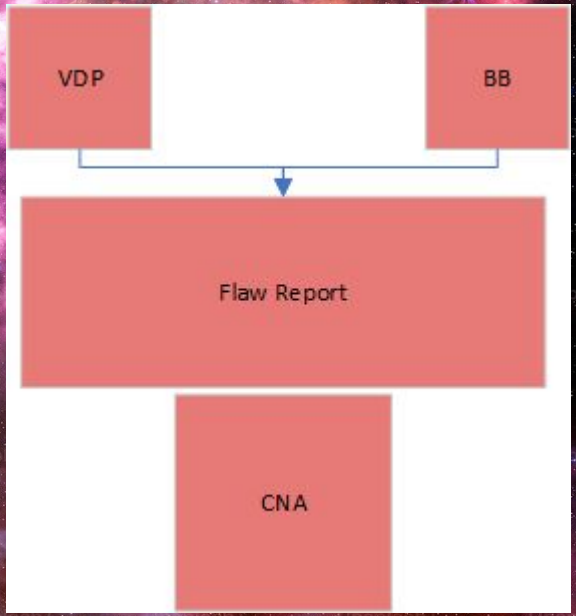



THIS WILL ALL
END IN TEARS


Flaw Report
Issue Analyzed
Fix creation/Coordination
Collateral created
Public Disclosure
View from up here....
A simple workflow illustrates what we'll be diving into

Flaw Report

The start of every vuln incident..... *Someone* finds *Something* and tells the *maintainer/owner** about it



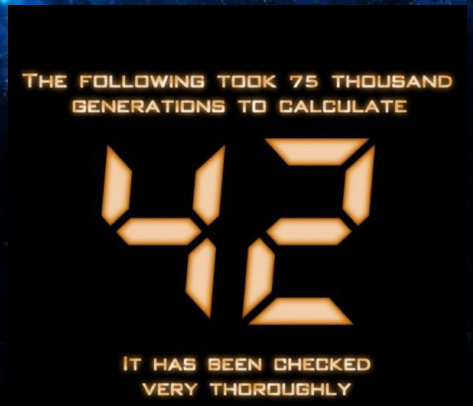
How does this stuff get found?

People

- Security Researchers
- Security Companies (Talos, etc.)
- Students
- Organizations
- Developers
- Community Maintainers
- Users
- 3V33L H@x0rs

How?

- Patching/Maintenance
- Development Lifecycle
- Pentesting/Fuzzing/Scanning
- By Accident

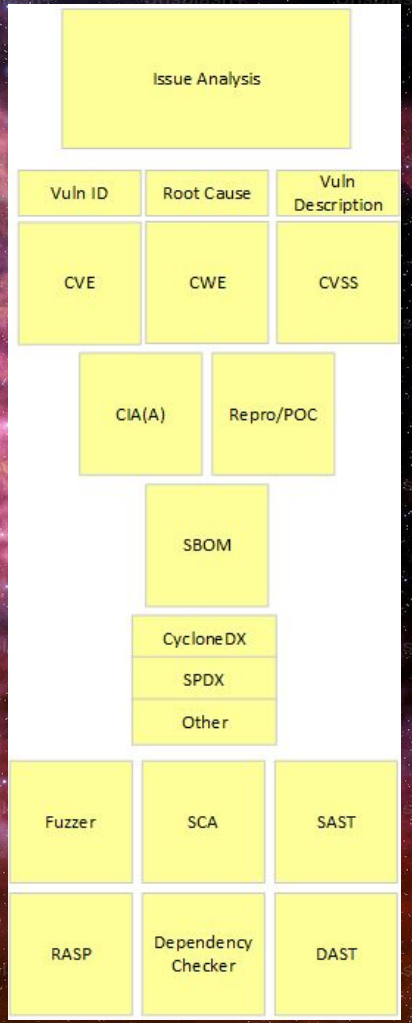


Terms - VDP & BB

- Stands for Vulnerability Disclosure Program/Process and Bug Bounty
- VDP stands for whatever intake process the maintainer uses to help collect defect reports
- Bug Bounty is a special form of VDP, where a 3rd party vendor manages vuln intake and pays out money based on the severity of the report

Issue Analysis

Once the report has been received, the hard work of understanding *WHAT* it is begins....



Flaw Analysis

The reports are reviewed by analysts that seek to understand what the problem is.

They seek to understand if the report Is valid or not.

They'll look to see if the issue has or needs a CVE assigned to it.

What is a CVE?

Terms - CVE & CNA

- Stands for ~~Common Vulnerabilities & Exposures~~ CVE
- It is a unique identifier for a specific problem.
- All CVEs are centrally coordinated by MITRE & their delegates (CNAs - CVE Numbering Authority).
- It allows researchers and maintainers the ability to have a common language used to describe vulnerabilities no matter what the platform.

https://cve.mitre.org/about/

CVE in-depth

CVE-2017-42

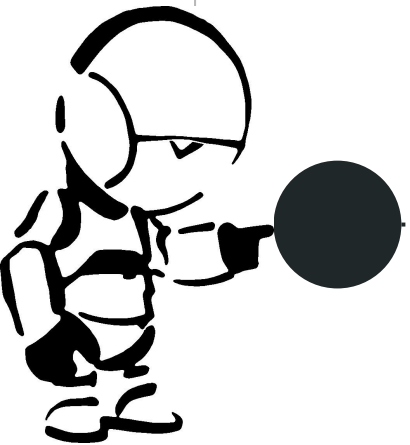
CVE's all contain a unique identifier

CVE's all contain a brief description

A flaw in the memory manager of the Babel Fish could allow a malicious attacker to change output from the Babel Fish's translation

CVE's all include relevant references

Megadodo Industries Bug Tracker: 42
www.md.org.net.com/bz=42.htm



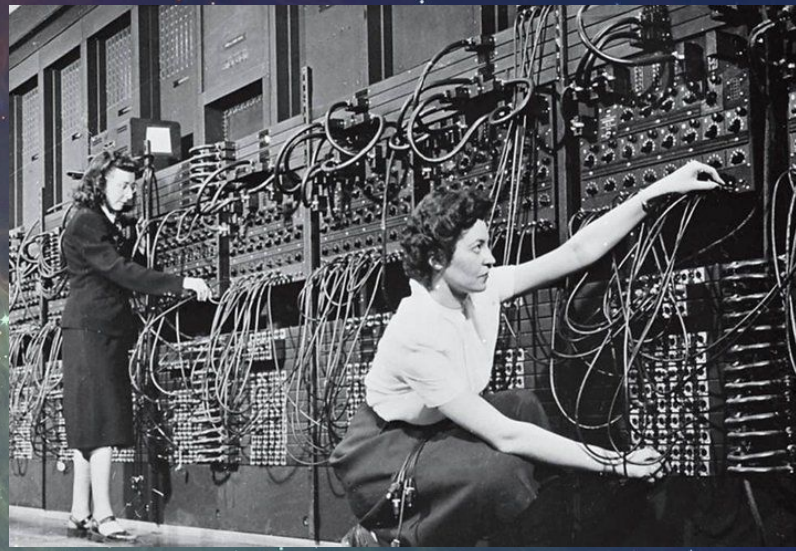
I guess I'll go read more about this.

Flaw Analysis, continued

The vulnerability gets a CVE identifier (or already has one).

Next the analyst will look to see what the reasons are for the flaw and assign a CWE.

What is a CWE?



Term - CWE

- Stands for Common Weakness Enumeration
- It is a unique identifier for a specific coding flaw.
- It allows developers and security practitioners to have a common language used to describe the weakness.
- Provides a baseline standard for weakness identification, mitigation, and prevention efforts.

https://cwe.mitre.org/about/index.html

CWE in-depth

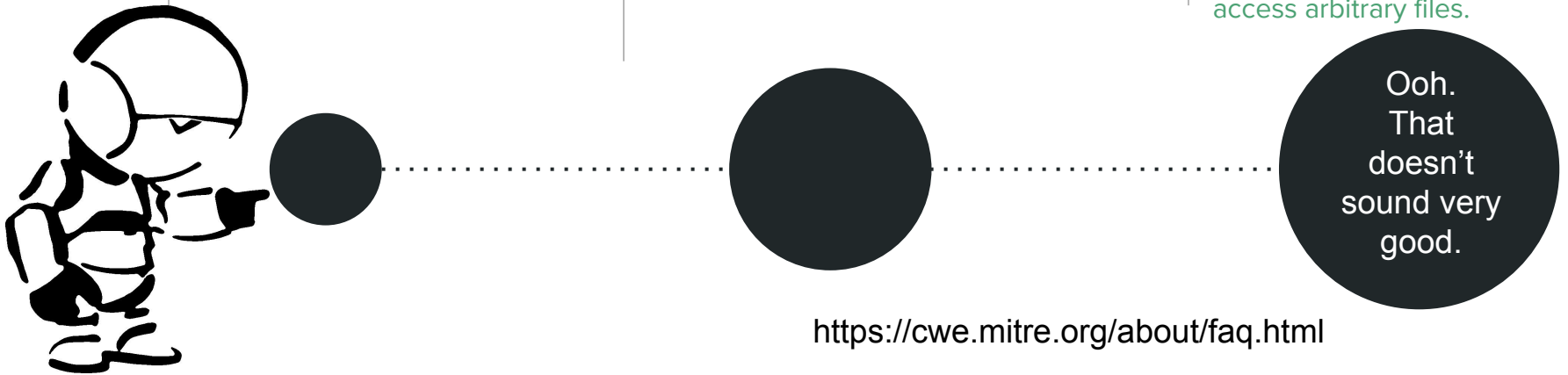
CWE-42 - Path Equivalence: ‘filename.’ (Trailing Dot)

What is a “software weakness”?

This is a problem within a software’s architecture, design, code, or implementation that if left unaddressed could result in systems being vulnerable to attack.

What does that mean?

A software system that accepts path input in the form of trailing dot ('filedir.') without appropriate validation can lead to ambiguous path resolution and allow an attacker to traverse the file system to unintended locations or access arbitrary files.



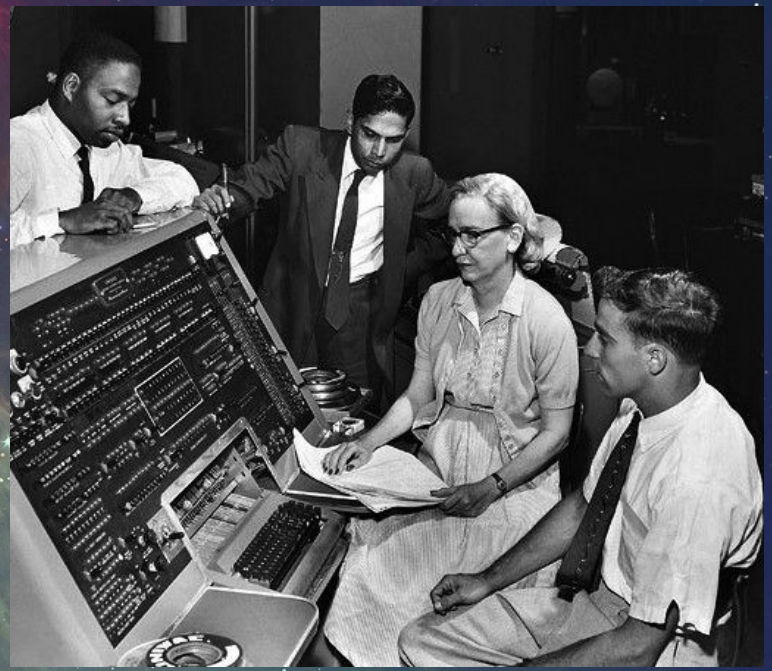
https://cwe.mitre.org/about/faq.html

Flaw Analysis, continuing to be continued

At this point we know how to talk about the problem (CVE) and what the fundamental coding problem is (CWE).

Next the analyst will work to understand how bad this thing is. The most common method of scoring flaws is CVSS.

What is a CVSS?



Term - CVSS

- Stands for Common Vulnerability Scoring System
- It is a methodology to capture characteristics of a vulnerability and produce a numeric score to reflect its severity.
- Again, this allows researchers and maintainers the ability to have a common language used to describe vulnerabilities and how severe the issue is.

https://www.first.org/cvss/

How to score using CVSS

Determine the base score

There are 17 dimensions of the flaw to review:

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction
- Primary Confidentiality
- Primary Integrity
- Primary Availability

Each is rated (mostly) on a High-Low-None scale

- Secondary Confidentiality
- Secondary Integrity
- Secondary Availability
- Safety
- Automatability
- Recovery
- Value Density
- Vulnerability Response Effort
- Provider Urgency

Those playing on the “Expert Level” could also look at these aspects of the issue

Environmental Modified Base Metrics

- Exploitability Metrics (AV. MAC, MAT, MR, M
- Vulnerable System impacts (CIA)
- Subsequent System Impacts (CIA)

Environmental Security Requirements

- System Impacts (CIA)

Threat Metrics

- Exploit Maturity

So I can modify the severity based off of *MY* environment. I guess that could be useful.

https://www.first.org/cvss/

What does a CVSS Score look like?

CVSS Score: 8.7/High ← This is the score for the issue. Oh dear, it sure looks pretty bad. I wonder **why** that is….

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:N/SA:L/S:N/AU:Y/R:U/V:D/RE:M/U:Green

- This is the version of CVSS used to score this flaw
- So the attack comes across the network
- Oh. The attack isn't very hard to execute
- There are some requirements that are need to exploit the vuln
- It doesn't need any local privileges
- The attack requires some passive action from the user
- So the Confidentiality, Integrity, and Availability of files can be completely compromised. That doesn't sound good at all.
- On secondary systems (after initial compromise), Confidentiality is completely compromised, Integrity is not affected, and Availability is affected at a Low level
- There are Negligible impacts on Safety
- An attack is Automatable
- Recovery of an affected system requires manual user intervention
- The resources that an attack would gain access too are limited
- The Response Effort level is moderate
- The provider advises this vulnerability has reduced urgency

https://www.first.org/cvss/calculator/4.0

Flaw Analysis, continuing the continuation to be continued

Now that the vuln is better understood the org needs to determine where that vulnerable component might be within their project, product, or platform

Tools like Software Bill of Materials (SBoM) are useful in that analysis

What is an SBoM?

Term - SBoM

- Stands for
  Software Bill of Materials
- This is a machine-readable artifact that collects all of the components and dependencies included with a piece of software or product.
- SBoMs should enable orgs to quickly see a list of components and versions included within software and be able to compare that to known CVE lists to understand what actions may need to be taken after a vuln report

https://www.cisa.gov/sbom

SBoM “Fun Facts”

Multiple formats

There are 3 formats to generate and share SBoMs::

- SPDX
- CycloneDX
- SWID

https://www.ntia.gov/sites/default/files/publications/sbom_formats_survey-version-2021_0.pdf

Multiple types based on when it was generated and who is using it

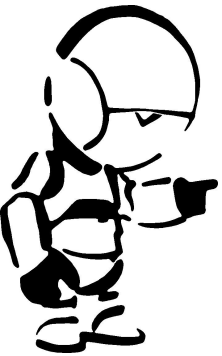
- Design
- Source
- Build
- Analyzed
- Deployed
- Runtime

https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

At its core, an SBoM share share these baseline elements

- Author Name
- Supplier Name
- Component Name
- Version String
- Component Hash
- Unique Identifier
- Relationship

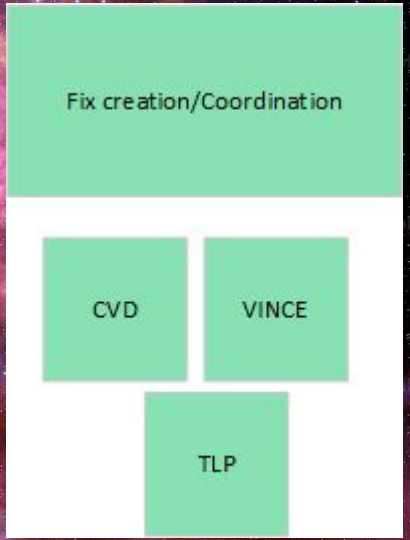
https://www.ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf



Wow, I suppose these could help me find out where my vulns are more quickly

Fix Creation/Coordination

Once there is a positive triage, and the flaw is understood, steps are taken to ensure that people authorized with “*need-to-know*” are read into the incident



Create and Test Fixes (finally)

The organization will begin working on resolving the flaw with a combination of knowledge articles, mitigations and code fixes.

However, sometimes the decision is made to embargo a flaw and not immediately publish any information about it.

What is an Embargo?

Term - Embargo

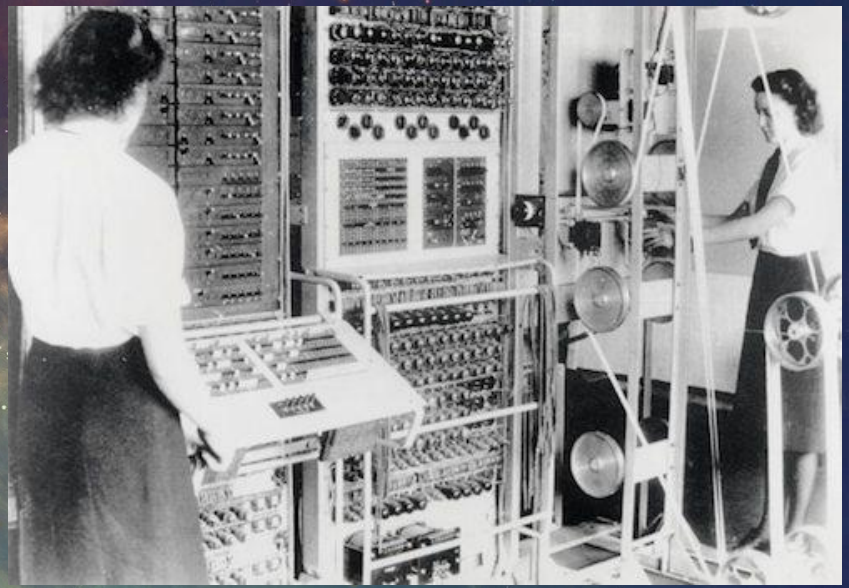
- A time period where vendors have access to details concerning the vulnerability, with an understanding not to publish these details or the fixes they have prepared.
- The reporter sets a date and time to lift the embargo, after which the information is considered public.
- The embargo ends with a Coordinated Release Date (CRD)/Public Disclosure Date (PD).
- Sometimes embargos are broken. This is generally considered a Bad Thing...

Coordination

Oftentimes, the maintainer needs additional people to assist in developing, testing, and distributing the fix.

These outsiders have “Need to Know” because they can directly contribute to the remediation

What is a CVD?



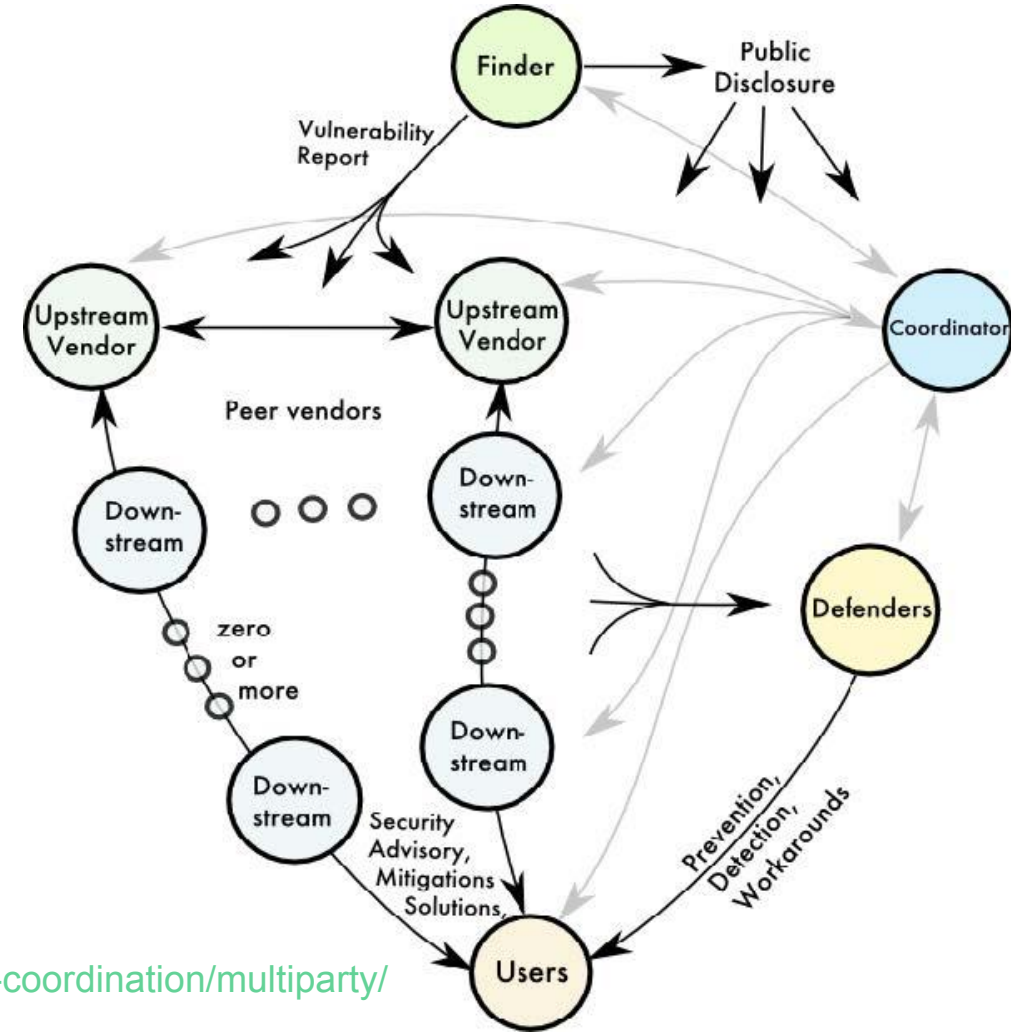
Terms - CVD

- Stands for Coordinated Vulnerability Disclosure
- This is the process of assembling the right people to help evaluate the vuln, create fixes to address it, and help stage and distribute the fixes when they are ready

https://www.first.org/global/sigs/vulnerability-coordination/multiparty/

CVD

CVD comes in many flavours, and depending on your place within the supply chain will determine how and when you may get included

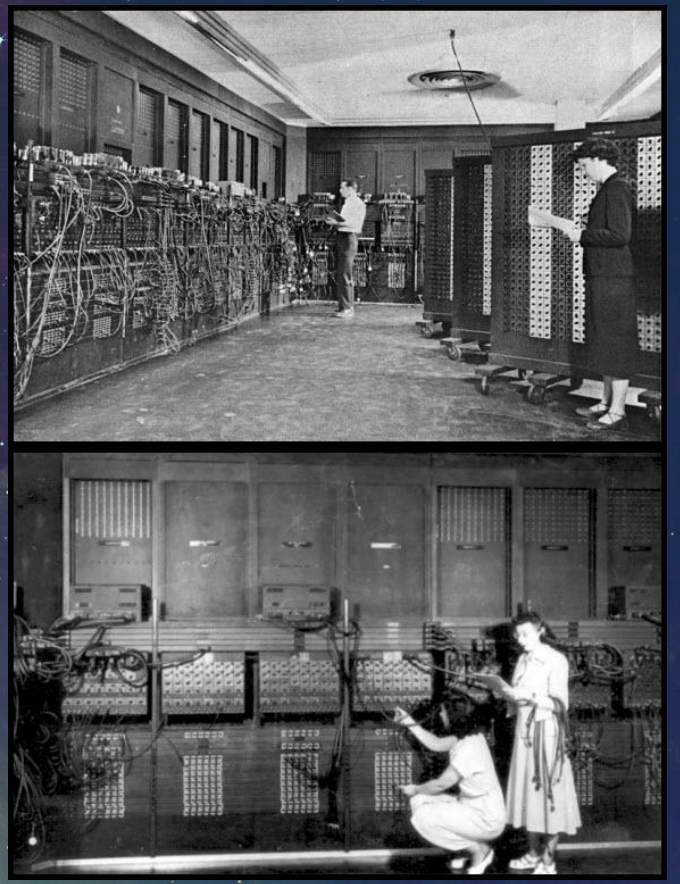


https://www.first.org/global/sigs/vulnerability-coordination/multiparty/

Disclosure, continued

To help advise readers on what they can share when working on an embargoed issue,you will often seen the materials labeled with a “TLP” colour

What is a TLP?



Term - TLP

- Stands for Traffic Light Protocol
- TLP encourages information sharing with and among public and private sector security professionals
- Colour-coded categories display with whom and how the included information can be shared (or not)

https://www.first.org/global/sigs/tlp/

TLP in-depth

TLP:RED

For the eyes and ears of individual recipients only, no further disclosure.

TLP:AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.

TLP:GREEN

Limited disclosure, recipients can spread this within their community.

TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure.

https://www.first.org/tlp/

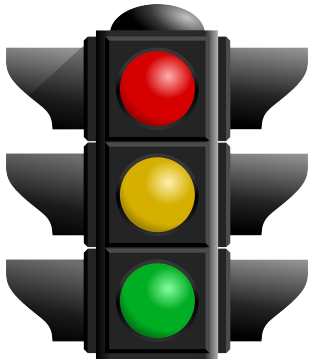
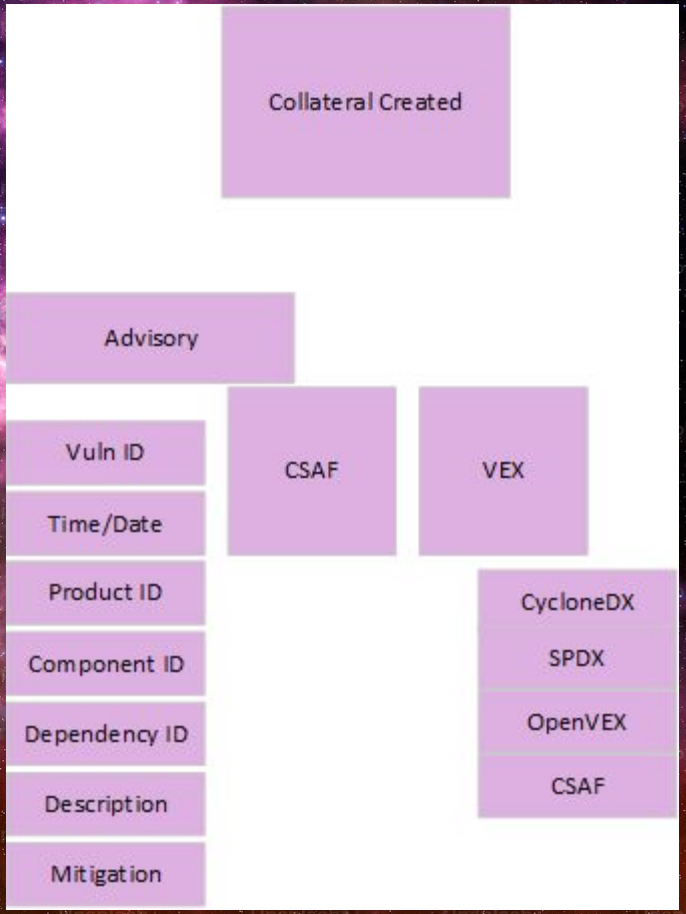


Image Source

Collateral Creation

As the patches near completion, the maintainer creates artifacts to inform the public & downstream about the issue



Informing downstream & the public

With the fixes complete and ready, now that information and how to address the problem needs to be shared so that consumers of the software can take action.

What is a Advisory?

Terms - Security Advisory

- Sometimes referred to as a VDR (Vulnerability Disclosure Report)
- A Security Advisory is the means by which an organization publicly discloses information related to the vulnerability
- CSAF (Common Security Advisory Format) is a machine-readable format that is broadly used by vendors to publish their advisories
- Platforms like GitHub allow the use of GSA (GitHub Security Advisory) allow software housed within their repo to use this format

https://oasis-open.github.io/csaf-documentation/
https://github.com/advisories

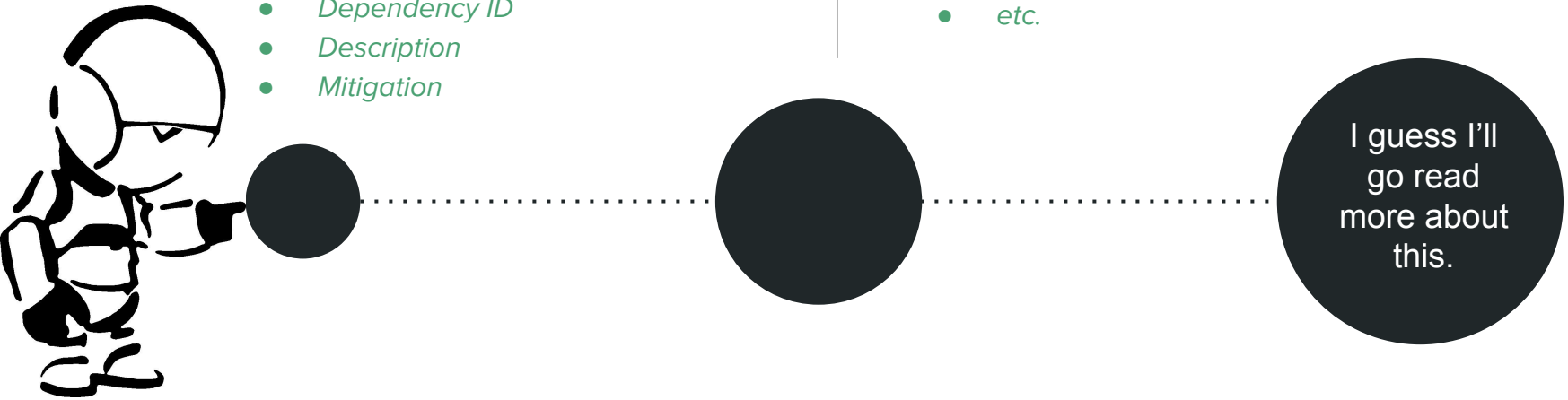
Security Advisories

A machine-readable format that should include the following pieces of data:

- *Vuln ID*
- *Time/Date*
- *Product ID*
- *Component ID*
- *Dependency ID*
- *Description*
- *Mitigation*

CSAF can integrated with other data elements like:

- *SBoM*
- *VEX*
- *EPSS*
- *KEV*
- *etc.*



Notifications & Advisories (yay!)

If a flaw is not under embargo, organizations will usually release an official statement about the vulnerability and if / how it affects their products, as well as any mitigations that do not require a patch.

Once fixes have been created and tested, the organization will release an advisory, containing a patch for one or more products. Typically these are published to organizational knowledge bases and mailing lists, and might also be sent to targeted groups of users.

Advisories are usually digitally signed by the organization to verify their legitimacy.

Collateral, continued

An advisory shares details about a vulnerability (name, CVE ID, etc.). It may often link to additional collateral (blogs, whitepapers, etc.)

An emerging framework to share additional information about the affectedness

What is a VEX?

Term - VEX

- Stands for Vulnerability Exploitability eXchange
- This is a Statement that asserts how and if a component is affected by a vulnerability

https://www.ntia.gov/sites/default/files/publications/vex_one-page_summary_0.pdf

VEX in-depth

VEX Statuses

- Not affected
- Affected
- Fixed
- Under Investigation

"Not affected" should provide details on:

- Component not present
- Vulnerable code not present
- Vulnerable code not in execution path
- Vulnerable code cannot be controlled by adversary
- Inline mitigation already exist

4 formats/tools

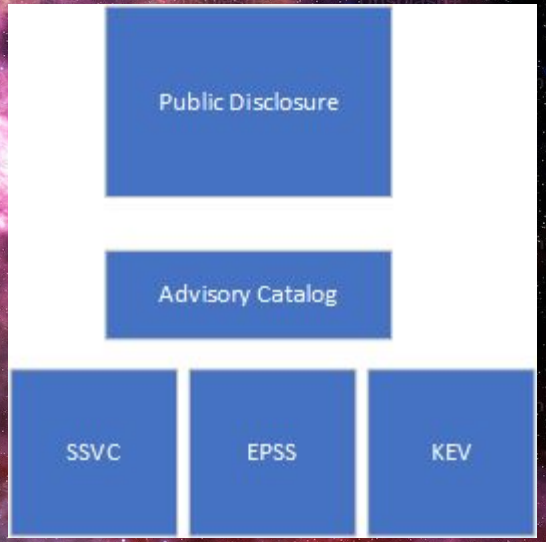
- CSAF
- CyCloneDX
- OpenVEX
- SPDX

I bet this could help reduce of lot of the noise from vuln scanners!

https://www.cisa.gov/sites/default/files/2023-11/When-to-Issue-a-VEX-508c.pdf
https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf

Public Disclosure

The patches and other public collateral is ready to be shared with the world.



Vulnerability Databases/Advisory Catalog

At Public Disclosure (PD) as advisories are published, they will appear on vendor/project websites, mailing lists, blogs, and social media

Several groups collect, aggregate, and more broadly share this information, such as the NVD

What is the NVD?

NVD - the big vulnerability dictionary in the cloud....

- NVD is the National Vulnerability Database and is maintained by the National Institute of Standards and Technology (NIST) [part of the US Department of Commerce]
- It is a database of enhanced CVE content
- It focuses on components that are used within the US.gov
  - So not ALL vulns will get coverage
- NVD can be incomplete or out of synch
- THE best source for information on a CVE is the vendor or team that supports that technology

https://nvd.nist.gov/

Expert Vuln Metadata

There are some additional, “Expert Level” frameworks and tools that are used to help consumers better understand the potential risks related to a vulnerability....

What is a EPSS?

Term - EPSS

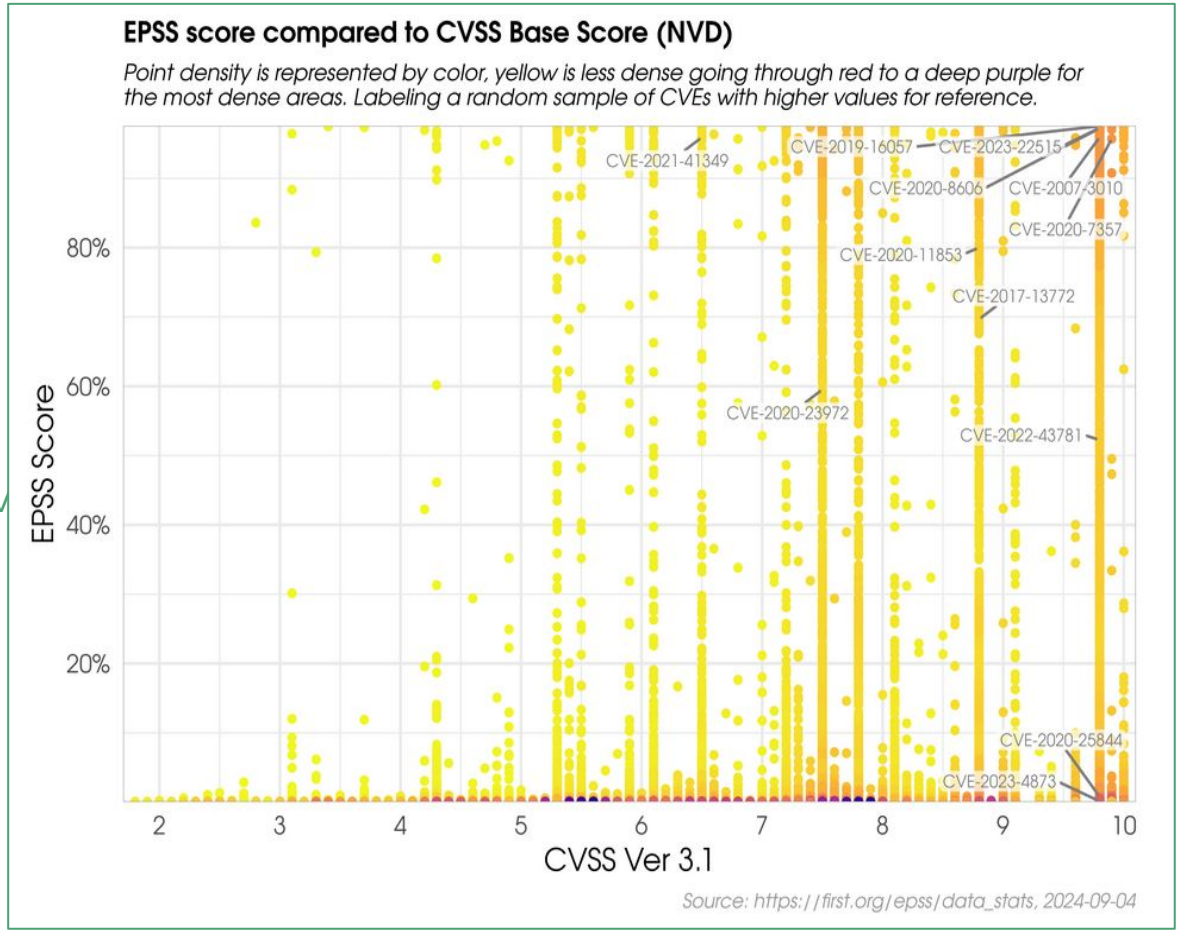
- Stands for Exploit Prediction Scoring System
- This is a data-driven effort to help quantify and estimate the probability that a vulnerability will be exploited based on historic vuln incident metadata
- This can be useful in trying to prioritize the never-ending stream of new CVEs you need to triage to decide how quickly to apply updates

https://www.first.org/epss/

EPSS in-depth

EPSS data

- Vendor (CPE, via NVD)
- Age of the vulnerability
- References with labels
- Normalized vuln descriptions
- Weakness of the vuln (CWE)
- CVSS Base metrics
- CVE has been reported exploited (KEV
- Publicly available exploit code
- Vuln integrated into security scanners



https://www.first.org/epss/model

Term - SSVC

- Stands for Stakeholder Specific Vulnerability Coordination
- SSVC is a decision-tree-based vuln analysis methodology that takes vuln exploitability, safety aspects, and install base into account
- This becomes a nice compliment for blue teamers to assists in apply their own security controls, requirements, and critical systems info into the accounting of how to prioritize vuln remediation

https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

SSVC in-depth

Five possible values

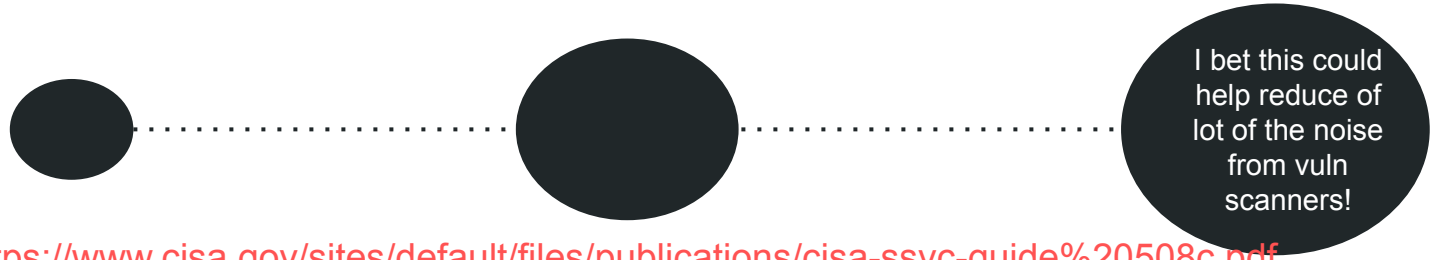
- **Exploitation status**
- **Technical impact**
- **Automatable**
- **Mission Prevalence**
- **Public well-being impact**

“Not affected” should provide details on:

- Component not present
- Vulnerable code not present
- Vulnerabile code not in execution path
- Vulnerabile code cannot be controlled by adversary
- Inline mitigation already exist

Four possible decisions

- **Track** - no action needed at this time
- **Track*** - Vuln has certain characteristics that require more attention
- **Attend** - Vuln should be addressed with normal patching timelines
- **Act** - Vuln should be addressed immediately



https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf
https://www.cisa.gov/ssvc-calculator

Term - KEV

- Stands for Known Exploited Vulnerabilities
- The authoritative source of exploited vulnerabilities for components the US.gov uses
- Everything on this list has been observed to be used in active exploits in the wild, so these are all very important to address as quickly as possible!

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

KEV in-depth

KEV deets

- In an advisory-style format (in CSV or json)
- Again, everything on this is has been observed in actual attacks and should be prioritized to be remediated as soon as possible
- This does not cover ALL SOFTWARE, so additional intel sources may be needed for coverage for software/hardware YOU use!

LINUX | KERNEL

CVE-2022-0185

Linux Kernel Heap-Based Buffer Overflow Vulnerability: *Linux kernel contains a heap-based buffer overflow vulnerability in the legacy_parse_param function in the Filesystem Context functionality. This allows an attacker to open a filesystem that does not support the Filesystem Context API and ultimately escalate privileges.*

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

- **Date Added:** 2024-08-21
- **Due Date:** 2024-09-11

Additional Notes +

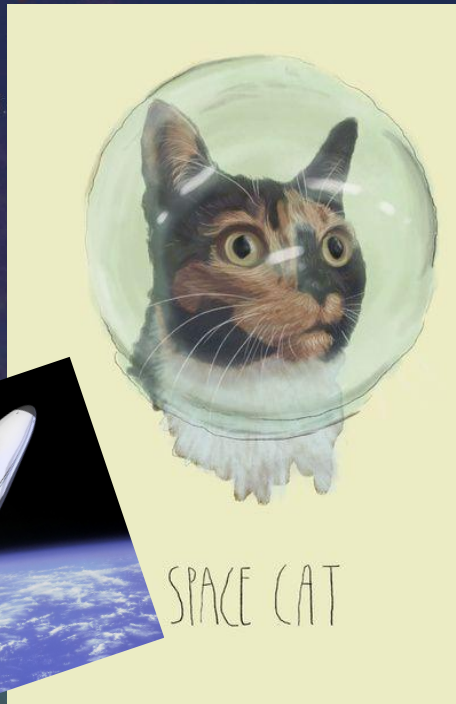
https://www.cisa.gov/sites/default/files/2023-11/When-to-Issue-a-VEX-508c.pdf
https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf

A few last things...

Support Life Cycles
Open Source Tracking

Why do they call it a lifecycle if nothing ever dies?

- Nothing is supported forever. (sorry)
- Be sure to understand how your vendor/community of choice supports components/applications you use.
- Most providers will provide “all” fixes for a set period of time, then gradually start to only fix the most severe things as the product ages. READ THE FINE PRINT to understand what support you are entitled to!

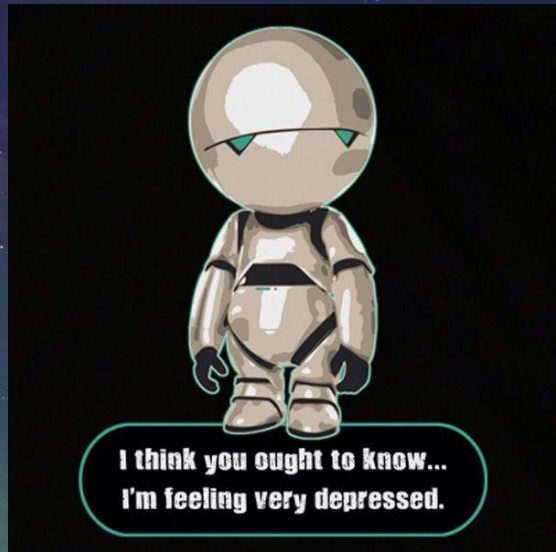


Who fixes Open Source?

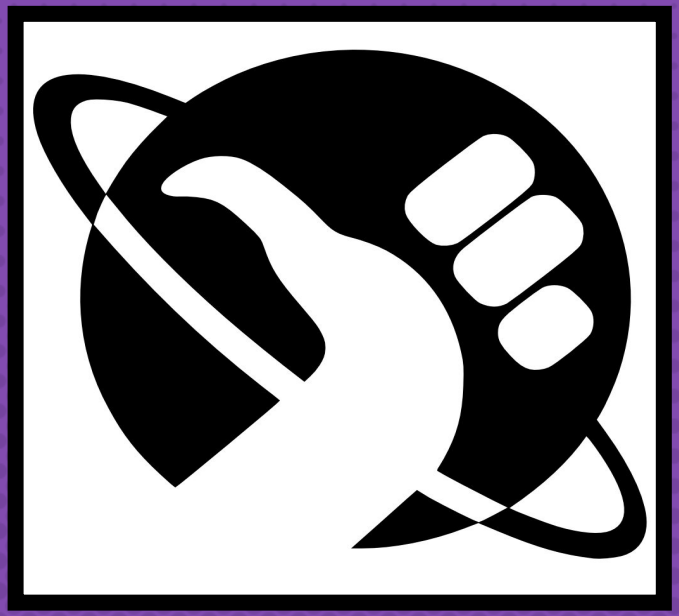
- There is no “The Open Source”. Each package/project/product can be managed by different types of people.
- We’ll take a moment to talk about a few types and something to help you out.

Summary - ZOMG so many letters and words!!!

- Security is not easy, but it is important.
- There are existing systems and processes in place to assist securing your applications.
- Knowing IS half the battle, the other half is using the available information to identify and mitigate vulnerabilities and potential threats.
- Leverage the offerings of your communities and vendors.



DON'T PANIC AND CARRY A TOWEL



Any questions?

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

@SecurityCRob

https://github.com/SecurityCRob

@SecurityCRob@infosec.exchange

The Security Unhappy Hour,
Chips & Salsa
What is in the SOSS