CVE framework

Definition. Framework for quantifying and categorizing the technical system vulnerabilities. This is a abbreviation from the common vulnerability evaluation framework..

Each organization, researcher or individual can report a vulnerability to a CVE institution which aggregates the repository of know vulnerabilities. CVE maintains the list of partner organizations on this page. Here is a short list of the process which goes before the cve is reported

- Discover vulnerability. Organization or individual
- Report a vulnerability to a CVE
- Request a CVE ID
- Reserve CVE ID
- Submit report
- Download it from public websites

Usually there are numerous ways how one could assign some measure to the vulnerability of some system. It is subjective and domain dependent. You could say that vulnerability is number of people it affects, you can do it by the importance of the people who does it affects.… The result score is the number between 0 and 100. It is classified into 5 categories.

CVSS v2.0 Ratings		CVSS v3.x Ratings	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Score is calculated based in 4 metrics;

- Base
- Threat
- Environmental
- Supplemental

Base score. How dangerous the vulnerability is ceteris paribus all other factors. In other words, one could say that this is how intrinsically dangerous the vulnerability is.
For example, Every one in the world have roughly the same probability to get a flue like diesese. So you put a universal score for some flu. Perhaps, this will not change over time and environment.
Temporal score. Characteristics of the vulnerability that change over time. For example, probability that child will die during birth is lower today than 100 years ago. We say that temporal metrics is lower.
Environmental. It is specific to the environment where the system is deployed.
Supplemental: additional description which cannot be classified in previous three. This is not quant measure.

Further information about evaluation specification could be found here.

One can find the taxonomy for assigning and evaluating attributes of the measures on this website link. With the score we also compress this evaluation to one string with the following format: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L

For example here is a description of the Base Metrics attributes.

- Attack Vector -> distance between "attacker and victim"
  - Network: attacker and targets are few network hops away and attack is happening the transport protocol layer
  - A: Adjacent
  - L: Local network
  - P: Physical distance
- Attack complexity
  - Complexity of the attack. Length of the supply chain or the action steps which need to be done to achieve the target. Each steps demands some amount of work and resources.
- Attack requirement
  - number of requirements which deployed system needs to satisy before action.
- Privileges required:
  - How many privelages should attacker have in order to break into system
- User Interactions:
  - How much should targeted user work in order that the mission is accomplished. For example, does user needs to have a very specific movements.
  - C: If the attack is successful, how much information can be attained? How much is confidentiality requirement affected?
  - I : How much can attacker change the system information. If someone breaks into your house and steals all your photographs will your memory disappear?
  - A : If the attacker breaks into vulnerable system how much is the system available to others and future attacks.

At the end of the assessment overall score is give to the product vulnerability. CVSS assessment is intended to be agnostic to the individual and their organization. Score should be objective and it should be a function of the ability of the attacker. Assumption is that attacker have an advanced knowledge of the target system and a default defense mechanism.

Questions and Answers

Give me a list of all CVE-s in 2024?
Here you go: link

Who published this?
d.cveMetadata.assignerShortName

I want to find out what products are affected by the latest cve?
d.containers.affected.vendor
d.containers.affected.product
d.containers.affected.platforms

How important the vulnerability is?
d.containers.metrics
Score is a function of the base, environment, temporal attribute scores.
The taxonomy where one can can find this is on this is here link

Ok, now I know what product is affected, how to defend or attack?
There are numerous frameworks which describe the tactics and strategies for organizing the attacks in more details. Some of them which I have found are here:

- MITRE: https://attack.mitre.org/
- OWASP Mobile: https://mas.owasp.org/
- Tools for mobile phone safety: https://mas.owasp.org/MASTG/tools/#android-tools

In Conclusion
A CVE dataset could be used for assessing the risk of the equipment which organization owns and to create statistics based alert system on various channels which could notify the asset owners about latest trends in the security community. The could be connected with other information sources such as MITRE attack framework for creating an steps needed to defend the equipment.