Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities

The Future of CVE

Global Security Vulnerability Summit 2022

Art MANION
amanion@cert.org
@zmanion

https://tinyurl.com/ysyd9fkt

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM22-0568

CERT Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University

- Coordinated vulnerability disclosure

CVE Board member

CVE Numbering Authority (CNA)

Cybersecurity & Infrastructure Security Agency (CISA)

Spirit of CVE past

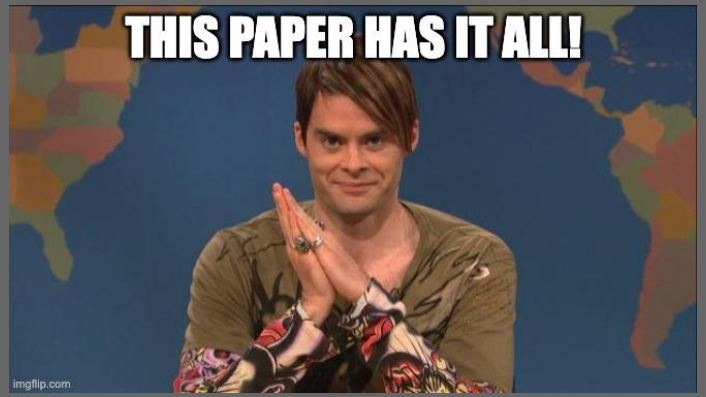
Towards a Common Enumeration of Vulnerabilities

David E. Mann, Steven M. Christey

The MITRE Corporation

202 Burlington Rd., Bedford MA 01730

January 8, 1999



Definition, abstraction, precision, boundary/bridge, minimalism, modularity, relationships

Spirit of CVE present

Services v2.0

- ID Reservation (IDR)

GitHub submissions

- https://github.com/CVEProject/cvelist

JSON v4.0

CVE automation

Services v2.1

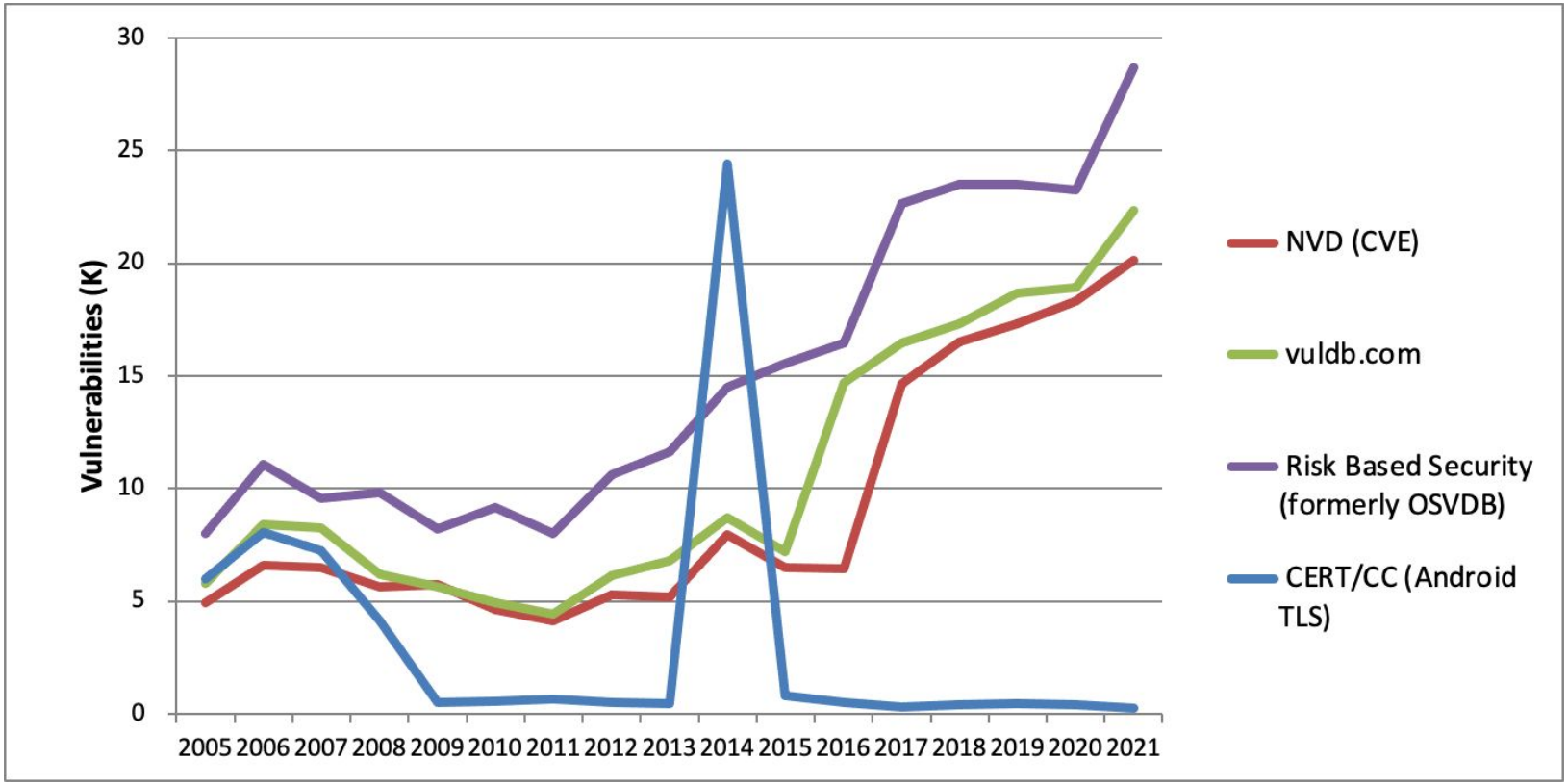
- ID Reservation (IDR)
- Record Submission and Upload Subsystem (RSUS)
- User Registration and Management Subsystem

JSON v5.0

- Upconversion
- Containers to support multiple sources
  - CNAs: Vendor, researcher, other?
  - ADP: Authorized Data Publisher, non-CNA, e.g., providing metrics or scoring data
- Better (more comptable) package, product, version formats

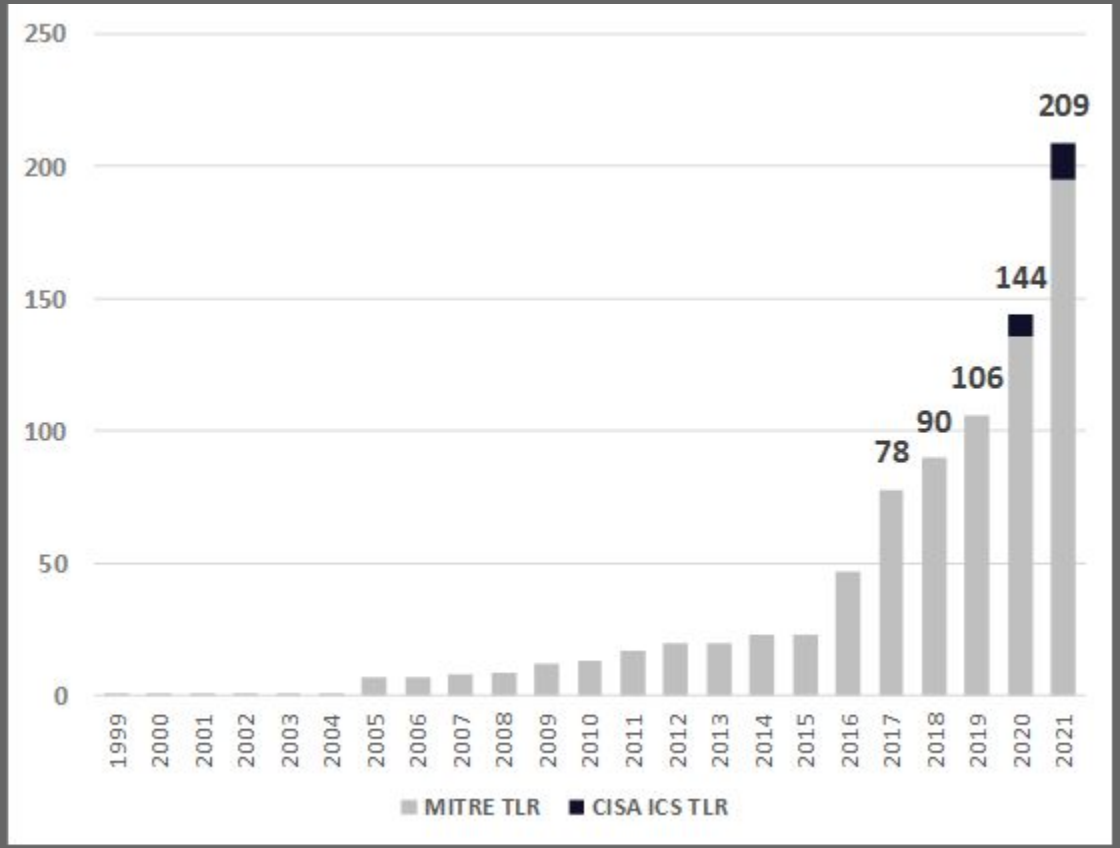
https://cveproject.github.io/automation-transition

Counting Vulnerabilities



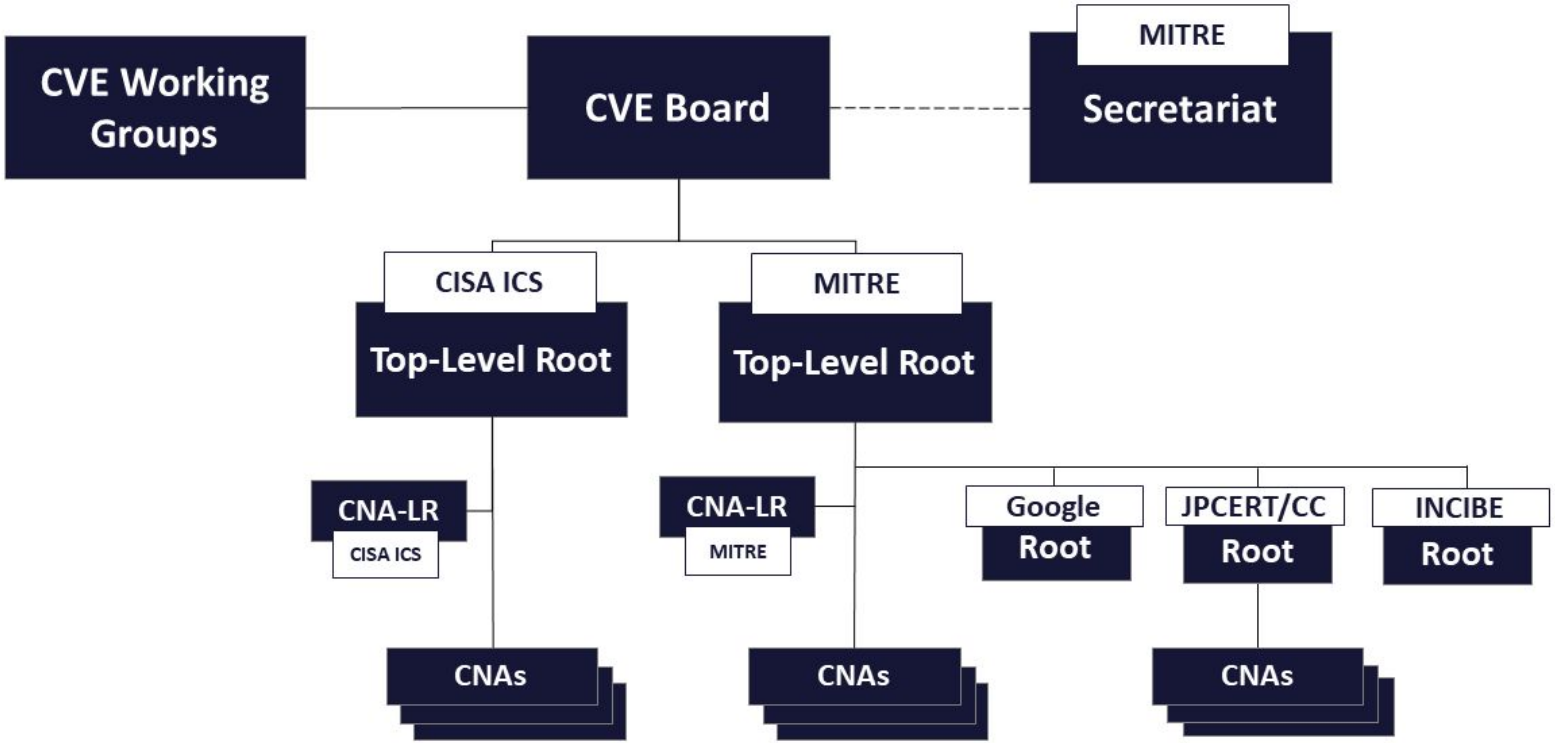
Counting CNAs

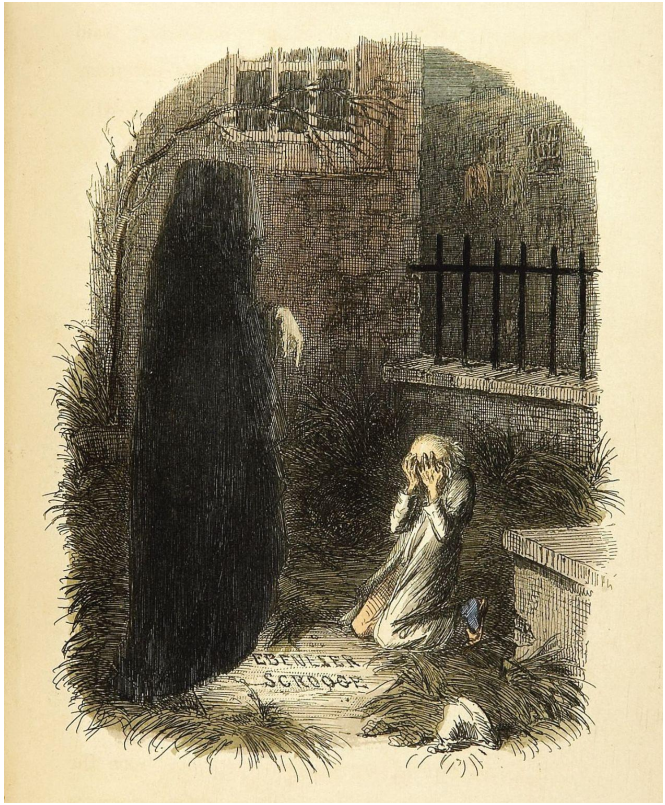
226 partners in 34 countries




CVE®
Partners
1-3
4-6
7-9
10-12
13-15
16+
United States · Australia · Austria · Belgium · Canada · China · Colombia · Denmark · Estonia · Finland · France
Germany · India · Ireland · Israel · Japan · Latvia · The Netherlands · New Zealand · Norway · Romania · Russia
Singapore · Slovakia · South Korea · Spain · Sweden · Switzerland · Taiwan · Turkey · United Kingdom · Vietnam

CVE Program Roles





Spirit of CVE future?

CVEs are dead, long live the CVE!

Greg Kroah-Hartman

Linux kernel dev: A bug is a bug

People using Linux: We'd like to know if that's a security bug…

Why We Created the Global Security Database

Coverage issues

PT-7528 and PT-7828 Series Ethernet Switches Vulnerabilities

Version: V1.0
Release Date: Sep 25, 2019
Reference:

- ICS-CERT, ICSA-20-056-03
- CVE-2020-6989, CVE-2020-6987, CVE-2020-6983, CVE-2020-6985, CVE-2020-6995, CVE-2020-6993
- CNVD-2020-13511, CNVD-2020-13512, CNVD-2020-13513, CNVD-2020-13514, CNVD-2020-13507

Multiple product vulnerabilities were identified in Moxa's PT-7528 and PT-7828 Series Ethernet Switches. In response to this, Moxa has developed related solutions to address these vulnerabilities.

EDS-405A Series Ethernet Switches Vulnerabilities

Version: V1.0
Release Date: Nov 07, 2019
Reference:

- CNVD-2019-116145, CNVD-2019-122728

Multiple product vulnerabilities were identified in Moxa's EDS-405A Series Ethernet Switches. In response to this, Moxa has developed related solutions to address these vulnerabilities.

Mission focus

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities

Less is more? More is more?

JSON 5.0 supports a lot of additional information

- CVE ID is not a vulnerability advisory?
- Should only contain minimum necessary information to identify and catalog?
- More information is debt?

“We argue that a vulnerability in a CVE does not need any attributes beyond a unique name and a textual description.” (1999)

Transparency

GitHub “pilot” will be replaced by RSUS

- A repository of CVE JSON files may be maintained
- Who changed what, when?
- CVE Board email is publicly archived
- Working groups vary

CVE is pro-transparency, implementation has scattered during growth

- A select few Board and secretariat communications are private

Mapping vulnerabilities to components

Three easy steps:

1. Identify all the components
2. Identify all the vulnerabilities
3. Map intersections

The first two are serious world-class problems and solutions probably involve distribution and/or federation

- Support (not) affected component lists directly in vulnerability formats?
- Graph/RDF?
- More computable version semantics
- VEX: Convey vulnerability status with “not affected because…” reasons

Disputes, updates

Follow CNA hierarchy

- Changes, updates, disputes are highly dependent on the authoring CNA
- Often ends up with a Top-Level Root CNA, usually MITRE

Cloud

7.4.5 CNAs MUST NOT assign a CVE ID to a vulnerability if the affected product(s) or service(s):

a. Are not owned by the CNA, and

b. Are not customer controlled.

Only a cloud service provider can assign for their services

CVE for malicious code?

CVE-2022-23812

- “…node-ipc from 10.1.1 and before 10.1.3…contains malicious code, that targets users with IP located in Russia or Belarus, and overwrites their files with a heart emoji.”

CVE for malicious code?

CVE-2018-3779

- “active-support ruby gem 5.2.0 could allow a remote attacker to execute arbitrary code on the system, caused by containing a malicious backdoor. An attacker could exploit this vulnerability to execute arbitrary code on the system.”
- "The gem duplicates official activesupport (no hyphen) code, but adds a compiled extension."

CVE-2017-16044

- “‘d3.js’ was a malicious module published with the intent to hijack environment variables. It has been unpublished by npm.”
- “This is essentially malware, just served up via an official repository. Since that does not represent a vulnerability in a piece of software, it is my understanding that this would not meet the criteria for inclusion in CVE.”

CVE for vulnerabilities in malware?

malvuln.com

BACKDOOR.WIN32.JOKERDOOR

Weak Hardcoded Credentials
MD5: a6437375fff871dff97dc91c8fd6259f
MVID-2022-0531

BACKDOOR.WIN32.WOLLF.H

Unauthenticated Remote Command Execution
MD5: 867c6b432ccd4aa51adc5e2722a4b144
MVID-2022-0530

BACKDOOR.WIN32.AVSTRAL.E

Unauthenticated Remote Command Execution
MD5: 35f0d754f161af35241cb081c73ea6dd
MVID-2022-0529

Existential motivation

Distributed Weakness Filing (DWF)

Global Security Database (GSD)

Other vulnerability databases

- VulnDB and vuldb
- CNNVD and CNVD
- osv.dev
- Many more…

Community, collaboration

While there could be less friction, the CVE Program wants, considers, and acts on input

- CNAs
- Researchers
- Anyone
- Other vulnerability databases! https://github.com/CVEProject/cve-schema/issues/87

```
"xref": {
    "type": "object",
    "required": ["rel_type"],
    "OneOf": [
      {"required": ["location"]},
      {"required": ["record_id"]}
    ],
    "properties": {
        "rel_type": {
            "type": "string",
            "enum": [
                "possibly_related",
                "related",
                "not equal",
                "equal",
                "superset",
                "subset",
                "overlap"
            ]
        },
```

Predominantly supply chain relationships

- SBOM, dependency tracking
- Common use of OSS in proprietary software

“A mapping that only uses an "equals" relation will be limited in its completeness.” (1999)

- Standard relationship system https://github.com/FIRSTdotorg/vrdx-sig-vxref-wip

Photo by Emily Morter on Unsplash

Thank you!

Questions?

amanion@cert.org @zmanion

References

https://cve.mitre.org/cve/cna/CNA_Rules_v3.0.pdf

https://cve.mitre.org/data/board/archives/2018-08/msg00002.html

https://github.com/FIRSTdotorg/vrdx-sig-vxref-wip

https://cveproject.github.io/automation-transition

https://github.com/CVEProject/cvelist/commit/b855f905aa1353ff825d0a71906c193b1967e9af#comments