Relationships Between CVE IDs and Vulnerability Abstraction

CNA Summit May 2021
Art Manion
amanion@cert.org

What is a vulnerability for CVE purposes?

How do CVE IDs relate to each other? To external IDs?

How big of a problem is the lack of relationships?

How does adding relationships satisfy various tradeoffs, particularly costs and benefits?

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.

DM21-0472

Photo by Jon Butterworth on Unsplash

The CERT/CC CNA

Coordinated Vulnerability Disclosure since 1988

- Usually as a 3rd-party coordinator, sometimes as a researcher
- Focus on multi-party CVD
- CVE since 1999
- CNA and Board member
- FFRDC, CISA sponsorship

CERT/CC
Vulnerability assignment related to its vulnerability coordination role

CNA

National and Industry CERTs

Abstractions

What *is* a vulnerability?

7.1 What Is a Vulnerability?

The CVE Program does not adhere to a strict definition of a vulnerability. **For the most part, CNAs are left to their own discretion to determine whether something is a vulnerability**. Root CNAs may provide additional guidance to their child CNAs. This allows the program to adapt to definitions used in different industries, legal regimes, and cultures.

7.1.1 If a product owner considers an issue to be a vulnerability in its product, then the issue MUST be considered a vulnerability, regardless of whether other parties (e.g., other vendors whose products share the affected code) agree.

7.1.2 If the CNA determines that an issue violates the security policy of a product, then the issue SHOULD be considered a vulnerability.

7.1.3 If a CNA receives a report about a new vulnerability that has a negative impact, then the reported vulnerability MAY be considered a vulnerability.

Abstractions

What *is* a vulnerability?

Appendix A: Definitions

A vulnerability in the context of the CVE Program is defined by Section 7. Assignment Rules. In general, a vulnerability is defined as a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, OR availability. Mitigation of the vulnerabilities in this context typically involves coding changes but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)." **NOTE: CNAs are not restricted to using this definition of a vulnerability.**

Problems

Multi-party vulnerability causes

- Supply chain, dependencies
  - Vulnerability and exploitability are not necessarily transitive!

Abstractions

- Protocol or format specification
- Conceptual implementation
- Code implementation

Loss of information

Lack of information or time

vxref

Vulnerability ID cross reference

Stale, partially completed effort from FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG)

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

...but a simple concept and still applicable

Subject	Verb (relationship)	Object
CVE-2043-1234	Equal	CVE-2042-1011
CVE-2019-9515	Subset	VU#605641
VU#605641	Superset	CVE-2019-9515

Relationship types

Unknown (default)	**Unknown (default)**
Possibly related	~~Possibly related~~
Related	~~Related~~
Not equal	**Not equal**
Equal	**Equal**
Superset	**Superset**
Subset	**Subset**
Overlap	~~Overlap~~

Examples

HTTP/2, independent implementations create similar (the same?) vulnerabilities

https://vuls.cert.org/confluence/pages/viewpage.action?pageId=56393752

~23K Android apps don't validate certificates

https://docs.google.com/spreadsheets/d/1t5GXwjw82SyunALVJb2w0zi3FoLRIkfGPc7AMjRF0r4

Transparent HTTP proxies shouldn't trust HTTP headers

https://github.com/FIRSTdotorg/vrdx-sig-vxref-wip/blob/master/vxref/data/v03/vu435052_vxref_03.json