Designing structured metadata for CVE

Bart van Dongen

February 1, 2021

Supervisor:

Armijn Hemel

Introduction

- Common Vulnerabilities and Exposures (CVE)
- 1999
- Industry standard
- Free text format

Research question

What metadata or structure could be added to the CVE to get information more easily?

Sub questions:

- What is the current status of CVE sources, databases and structure?
- Which data is not properly accessed in the CVE?
- What tools are available for converting CVE reports for easier processing by machines?
- What additional data should the CVE contain?

Related work

Peter Mell and Tim Grance wrote three guidelines for federal organizations on the use of CVE vulnerability naming scheme.

David A. Waltermire and Karen Scarfone updated the “Guide to using vulnerability naming schemes”.

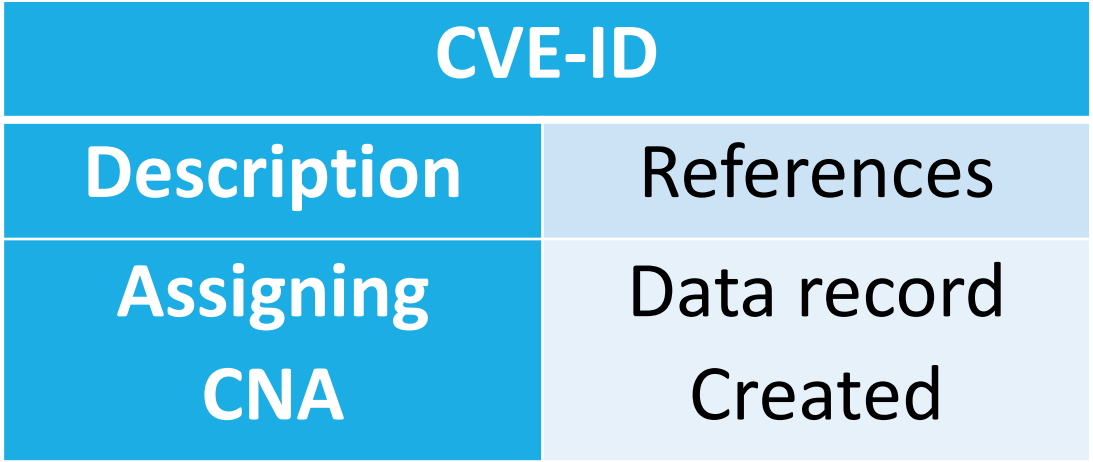
H.S. Venter, J.H.P. Eloff and Y.L. Li. used artificial intelligence to generate a standard set of vulnerability categories.

Methodology

- literature study
- Interviews

CVE status

- MITRE
- CVE numbering Authorities
- Structure



CVE databases

- NVD NIST
- VULDB
- Whitesource vulnerability database
- CIRCL

CVE Metadata

- Common Weakness Enumeration (CWE)
- Common Vulnerability Scoring System (CVSS)
- Common Platform Enumeration (CPE)

CVE description

Standard characteristics:

- Product
- Type of vulnerability
- What happens

CVE conversion tools

- Difficulty
- Machine learning

Missing data

- Product
- Fix
- Type of vulnerability
- SDK
- Manufacture
- Affected source code

New structure CVE

CVE-ID	
Description	References
Assigning CNA	Data record Created
CWE	CPE (AFFECTED version)
Fixed version	CVE version
***SDK**	*Manufacture
***File : lines**	

Conclusion

- Information
- New structure

Future work

- Form
- Tool

Questions