

cve-search - a free software to collect, search and analyse
common vulnerabilities and exposures in software



CIRCL

Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy and
Pieter-Jan Moreels

CC3C

29th December 2016

What are CVE's?

Common Vulnerabilities and Exposures

- Used by most important vendors
- **Unique** identifier for a vulnerability
- Issued by **MITRE**
- Stored in the **NVD** (National Vulnerability Database)
- Linked to products by **CPE** (Common Platform Enumerator)

Format: CVE-YYYY-NNNN

And CPE's?

cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:
{language}:{sw_edition}:{target_sw}:{target_hw}:{other}

part	name
o	Operating System
a	Application
h	Hardware

An empty part defines any element.

CPE 2.2 Format

cpe:/o:microsoft:windows_vista:6.0:sp1:~::~home_premium~::~x64~-

CPE 2.3 Format

cpe:2.3:o:microsoft:windows_vista:6.0:sp1:-:-:home_premium:-:x64:-

What is CVE-Search?

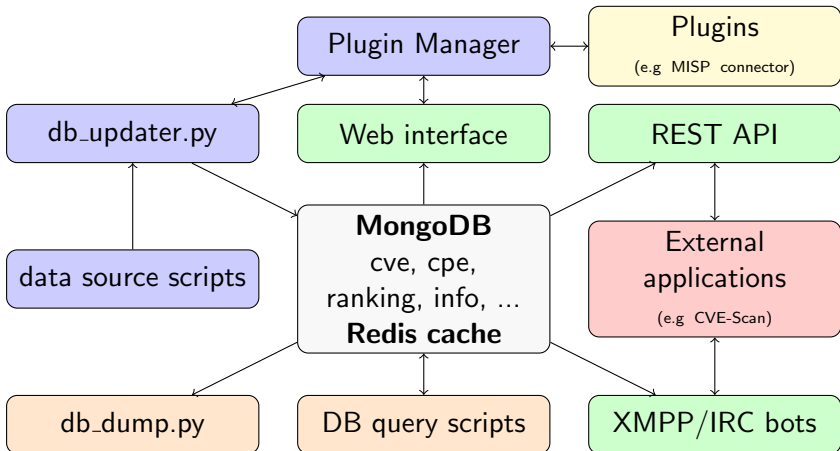
A framework to import **CVE** and **CPE** into a MongoDB and enrich this data with vulnerability information to facilitate search and processing of CVEs.

- **Offline** local search
- **Fast-lookup** of vulnerabilities information
- **Localized** classification of vulnerabilities
- **Enriched** information (e.i. NIST/NVD is not the only source).
- Allowing the use of **Unix-like tools** to process the vulnerabilities.
- **REST API** to integrate **custom tools**.

Sources

- **CVE** - NIST NVD
- **CPE** - NIST NVD
- **CWE** (Common Weakness Enumeration) - MITRE
- **CAPEC** (Common Attack Pattern Enumeration & Classification) - MITRE
- **VIA4** (Vulnerability Information Aggregator for CVE's)
 - D2sec
 - exploit-db
 - IAVM (Information Assurance Vulnerability Management)
 - Microsoft Bulletins
 - OVAL (Open Vulnerability & Assessment Language)
 - Redhat RPM & Advisories
 - MITRE Reference maps
 - Saint exploit information
 - MITRE Vendor statements
 - VMWare Security Advisories

A functional overview of cve-search





Unix-like tools to utilize this data

Select all CVEs with a score of 10, applicable to Joomla

```
$ python3 bin/search.py -p joomla: -o json | jq -r '
  select (.cvss=10.0) | .id '
CVE-2014-7228
CVE-2015-8769
CVE-2015-8562
... <truncated> ...
```

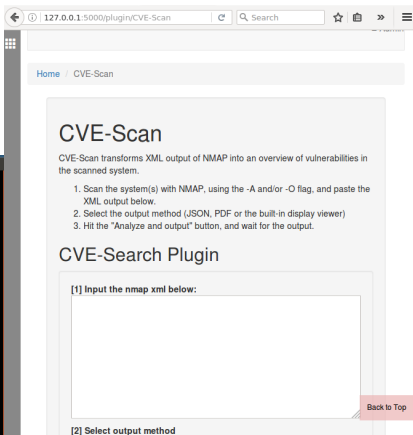
Visualization using the browser (index.py)

cve-search	Recent	Browse per vendor	Search CVE	search	Admin	+
Hide/Show filter						
« 4 5 6 7 8 »						
<input checked="" type="radio"/> Don't mark <input type="radio"/> Mark seen <input type="radio"/> Mark unseen						
ID	CVSS	Summary	Last (major) update	Published		
CVE-2015-0514	5.0	EMC M&R (aka Watch4Net) before 6.5u1 and ViPR SRM before 3.6.1 might allow remote attackers to obtain cleartext data-center discovery credentials by leveraging certain SRM access to conduct a decryption attack.	29-09-2015 - 02:34	21-01-2015 - 16:17		
CVE-2015-0158	4.3	Cross-site scripting (XSS) vulnerability in the Coach NG framework in IBM Business Process Manager (BPM) 8.0 through 8.0.1.3, 8.5.0 through 8.5.0.1, and 8.5.5 through 8.5.5.0 allows remote attackers to inject arbitrary web script or HTML via a crafted	29-09-2015 - 02:33	24-03-2015 - 03:01		
 CVE-2014-9403	4.0	The CWebAdminMod::ChanPage function in modules/webadmin.cpp in ZNC before 1.4 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) by adding a channel with the same name as an existing channel but withou	29-09-2015 - 02:31	19-12-2014 - 16:59		
 CVE-2014-8600	4.3	Multiple cross-site scripting (XSS) vulnerabilities in KDE-Runtime 4.14.3 and earlier, kwebkitpart 1.3.4 and earlier, and kio-extras 5.1.1 and earlier allow remote attackers to inject arbitrary web script or HTML via a crafted URI using the (1) zip,	29-09-2015 - 02:31	08-12-2014 - 12:59		
CVE-2014-7231	2.1	The strutils.mask_password function in the OpenStack Oslo utility library, Cinder, Nova, and Trove before 2013.2.4	29-09-2015 - 02:30	08-10-2014 - 21:55		

Using the API or plug-ins

```
File Edit View Search Terminal Help
IP          74.207.244.221
MAC         Unknown
Status      up
CPEs        cpe:/o:linux:linux_kernel:2.6.39
Vendor
Hostnames    scanme.nmap.org
             li86-221.members.linode.com
Distance    11
Services    ssh (22/tcp) is open
             > OpenSSH
             > cpe:/a:openbsd:openssh:5.3p1
             http (80/tcp) is open
             > Apache httpd
             > cpe:/a:apache:http_server:2.2.14

(u)p | (n)ext | (p)revious | (q)uit |
(d)own | (j)ump to | (c)ommand | (o)pen | [1/1]
```



Major recent changes

- Replaced vFeed by VIA4
- Plugin Manager
- Authentication Manager
- Gitter community

Roadmap

- Improve information feeds
- Modularize the code
- Rework internal structure for code maintenance
- Implement custom vulnerability identifier for non-CVE's

Contact Details

Pieter-Jan Moreels



@PidgeyL



@NorthernSec



pieterjan.moreels@gmail.com

Github	cve-search/cve-search
Website	CVE-Search.org
Online API	cve.circl.lu
Gitter.im	cve-search/cve-search