NVD 漏洞数据库说明

编制：赵辉

编制日期：2021.9.28

修订日期：2021.11.11

版本:V1.2

Contents

[1. 数据库说明 3](#_Toc55768089)

[1.1. 数据库名称 3](#_Toc991401731)

[1.2. 数据库格式 3](#_Toc163275844)

[1.3. 数据库字段类型 3](#_Toc1840492889)

[2. 数据表字段说明 3](#_Toc809534035)

[2.1. NVD数据表(主) 3](#_Toc1529622500)

[2.2. cve表 4](#_Toc838619263)

[2.3. problemtype表 5](#_Toc738777980)

[2.4. refs表 5](#_Toc2038546553)

[2.5. description表 5](#_Toc897812033)

[2.6. configration表 6](#_Toc1306734809)

[2.7. impact表 7](#_Toc2124160641)

[3. 数据爬虫使用说明 8](#_Toc999745559)

[3.1. 文件的获取 8](#_Toc811555985)

[3.2. 解压后会获得如下文件： 8](#_Toc1152797798)

[3.3. 程序的执行 9](#_Toc475127752)

## 数据库说明

## 数据库名称

数据库文件名为NVD.db。

## 数据库格式

数据库采用sqlite为基本数据数据存储，版本号3.0

## 数据库字段类型

本数据库中采用text做为主要数据存储类型，string,chat等类型均归于text类型。

日期相关类型包括time,date,datetime等在本数据库中采用date进行存储，如后期使用其它数据库，需求根据情况进行转换。

布尔形数据采用boolean数据类型存储，在数据值上表现为true=1，false=0

## 数据表字段说明

## NVD数据表(主)

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 说明 | 取值举例 |
| CVE\_data\_type | text | CVE数据类型 | CVE |
| CVE\_data\_format | text | CVE数据格式 | MITRE |
| CVE\_data\_version | text | CVE数据版本 | 4.0 |
| CVE\_data\_numberOfCVEs | text | 指示数据文件总记录条数，这里通常以年为单位 | 11398 |
| CVE\_data\_timestamp | date | CVE数据文件时间戳（sqlite里等同text字段，其它数据库需根据情况做转换） | 2021-09-27T07:00Z |
| problemtypeTid | text | CVE数据记录号，关联problemtype表的CVE\_ID键 | CVE-2021-0001 |
| referencesTid | text | CVE数据记录号，关联references表的CVE\_ID键 | CVE-2021-0001 |
| descriptionTid | text | CVE数据记录号，关联description表的CVE\_ID键 | CVE-2021-0001 |
| configurationTid | text | CVE数据记录号，关联configuration表的CVE\_ID键 | CVE-2021-0001 |
| impactTid | text | CVE数据记录号，关联impact表的CVE\_ID键 | CVE-2021-0001 |

## cve表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 说明 | 取值举例 |
| data\_type | text | CVE数据类型 | CVE |
| data\_format | text | CVE数据格式 | MITRE |
| data\_version | text | CVE数据版本 | 4.0 |
| CVE\_data\_meta\_ID | text | CVE数据记录号,与NVD主表关联 | CVE-2021-0001 |
| CVE\_data\_meta\_ASSIGNER |  | 数据提供人 | secure@intel.com |
| publishedDate | date | 公开日期 | 2021-06-09T20:15Z |
| lastModifiedDate | date | 最后修改日期 | 2021-06-28T18:03Z |

## problemtype表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 说明 | 取值举例 |
| CVE\_ID | text | CVE数据记录号 | CVE-2021-0001 |
| lang | text | 描述语言 | en |
| value | text | 描述 (CWE号） | CWE-203 (或类似NVD-CWE-Other) |

## refs表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 说明 | 取值举例 |
| CVE\_ID | text | CVE数据记录号 | CVE-2021-0001 |
| url | text | 漏洞公布链接 | https://www.debian.org/security/2021/dsa-4931 |
| name | text | 名称 | DSA-4931 |
| refsource | text | 影响源 | DEBIAN |
| tag | text | 标签（如有多个以，分隔） | Mailing List,Third Party Advisory |

## description表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 说明 | 取值举例 |
| CVE\_ID | text | CVE数据记录号 | CVE-2021-0001 |
| lang | text | 描述语言 | en |
| value | text | 漏洞描述 | Observable timing discrepancy in Intel(R) IPP before version 2020 update 1 may allow authorized user to potentially enable information disclosure via local access. |

## configration表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 说明 | 取值举例 |
| CVE\_ID | text | CVE数据记录号 | CVE-2021-0001 |
| CVE\_data\_version | text | CVE数据版本 | 4.0 |
| node\_level | int | 结点级别，同级别内容使用相同的逻辑操作符(operator) | 0  1  2 |
| operator |  | 逻辑操作符 | OR或 AND |
| vulnerable | boolean | 是否为漏洞(sqlite中以1和0表示） | 1 |
| cpe23Uri | text | CPE表达串，具体请参见CPE规则说明 | cpe:2.3:a:intel:integrated\_performance\_primitives\_cryptography:2019:-:\*:\*:\*:\*:\*:\* |
| cpe\_name | text | CPE名称（通常为空数据） |  |
| versionStartIncluding | text | 影响包含开始版本号 | 1.0.2 |
| versionEndIncluding | text | 影响包含结束版本号 | 2.03 |
| versionStartExcluding | text | 影响不包含开始版本号 | 1.2beta2 |
| versionEndExcluding | text | 影响不包含结束版本号 | 5.0.3 |
| cpe\_version | text | CPE版本号 | 2.3 |
| part | text | 类型a:应用，o：操作系统（包括固件），h：硬件（包括固件） | a |
| vendor | text | 厂家名称 | Microsoft |
| product | text | 产品名称 | Windows10 |
| version | text | 版本号 | 20h2 |
| update | text | 补丁号 | Sp1 |
| edition | text | 修正号 | enterprise\_server |
| language | text | 语言 | zh |
| sw\_edition | text | 软件版本 | enterprise |
| target\_sw | text | 目标软件 | macos |
| target\_hw | text | 目标硬件 | arm64 |
| other | text | 其它信息 | node.js |

\*：如遇以\*号表示字段，表明此字段为空

## impact表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 说明 | 取值举例 |
| CVE\_ID | text | CVE数据记录号 | CVE-2021-0001 |
| V3\_version | text | V3版本号（注：2014年后数据才有V3版本数据加入，之前为空数据） | 3.1 |
| V3\_vectorString | text | 引导字串 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N |
| V3\_attackVector | text | 攻击方式 | LOCAL，ADJACENT\_NETWORK |
| V3\_attackComplexity | text | 攻击复杂度 | LOW |
| V3\_privilegesRequired | text | 权限要求 | HIGH |
| V3\_userInteraction | text | 用户交换 | REQUIRED |
| V3\_scope | text | 范围 | UNCHHANGED |
| V3\_confidentialityImpact | text | 保密性影响 | HIGH |
| V3\_integrityImpact | text | 完整性影响 | NONE |
| V3\_availabilityImpact | text | 有效果性影响 | HIGH |
| V3\_baseScore | text | 基础评分 | 6.5 |
| V3\_baseSeverity | text | 严重性评分 | MEDIUM |
| V3\_exploitabilityScore | text | 暴露性评分 | 0.8 |
| V3\_impactScore | text | 影响性评分 | 3.6 |
| V2\_version | text | V2版本号 | 2.0 |
| V2\_vectorString | text | 引导字串 | AV:A/AC:L/Au:N/C:P/I:N/A:N |
| V2\_accessVector | text | 攻击方式 | LOCAL |
| V2\_accessComplexity | text | 攻击复杂度 | LOW |
| V2\_authentication | text | 身份验证 | NONE |
| V2\_confidentialityImpact | text | 保密性影响 | PARTIAL |
| V2\_integrityImpact | text | 完整性影响 | PARTIAL |
| V2\_availabilityImpact | text | 有效果性影响 | PARTIAL |
| V2\_baseScore | text | 基础评分 | 3.3 |
| V2\_severity | text | 严重性评分 | LOW |
| V2\_exploitabilityScore | text | 暴露性评分 | 6.2 |
| V2\_impactScore |  | 影响性评分 | 0.8 |
| V2\_acInsufInfo | boolean | 非充足信息访问(0=false,1=true以下类同) | 0 |
| V2\_obtainAllPrivilege | boolean | 获取全部权限 | 0 |
| V2\_obtainUserPrivilege | boolean | 获取用户权限 | 0 |
| V2\_obtainOtherPrivilege | boolean | 获取其它权限 | 0 |
| V2\_userInteractionRequired | boolean | 用户交互 | 0 |

## 数据爬虫使用说明

## 文件的获取

在指定的地方获取打包文件，并解压文件。

文件包含内容

## 解压后会获得如下文件：

crawl\_NVD\_linux: Linux下的执行文件

crawl\_NVD\_macos: Mac(m1)下的执行文件，x86架构版本未做测试

backup.sql: sqlite3使用的一次性清理NVD.db数据库文件。打开sqlite3 NVD.db

.read backup.sql 就可以完成数据的清除和数据空间的释放

req.txt 所需python第三方库文件列表，使用pip3.9 install -r req.txt进行安装

NVD.db 数据库文件，里面只有基本库结构，此文件必须有，否则程序不能执行

## 程序的执行

无论在Linux或者MacOS环境下，都确认执行文件有执行权限，并以./crawl\_NVD\_xxx来运行，再次提醒，同级目录下必须有NVD.db数据库文件存在。在执行过程中会提示下载和数据处理进度，等全部完成会，会产生data文件夹，包含所有.json的文件。 JSON格式数据已经全部进行NVD.db数据库。

注：1. 确保NVD.db数据库文件与执行文件在同一路径中。

2.目前只开放NVD.org站点的数据爬取JSON，日期从2002-2021年。CNNVD数据及xml数 据格式会相继开放，并以参数形式进行选择。