NVD 漏洞数据库说明

编制：赵辉

日期：2021.9.28

contents

[1. 数据库说明 3](#_Toc203987926)

[2. 数据表字段说明 3](#_Toc695335304)

[1) NVD数据表(主) 3](#_Toc807027349)

[2) cve表 4](#_Toc1986151888)

[3) problemtype表 4](#_Toc117986580)

[4) refs表 5](#_Toc2097342999)

[5) description表 5](#_Toc1035391628)

[6) configration表 5](#_Toc1602612186)

[7) impact表 6](#_Toc1258456612)

## 数据库说明

* 1. 数据库名称

数据库文件名为NVD.db。

* 1. 数据库格式

数据库𦠐采用sqlite为基本数据数据存储，版本号3.0

* 1. 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 |

## **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 |