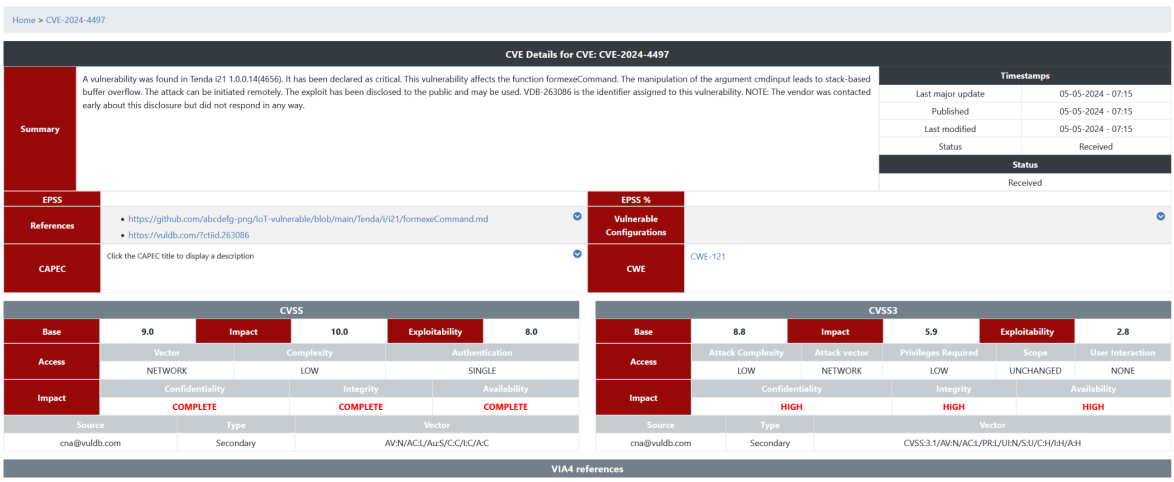
CVE库的使用手册说明

这两个导航选项的含义是：

- **Browse per vendor**：按供应商浏览漏洞 - 允许用户根据软件/硬件供应商（如Microsoft、Cisco、Oracle等）来筛选和查看相关的CVE漏洞记录。
- **Browse CWEs**：浏览通用弱点枚举 - 允许用户按CWE（Common Weakness Enumeration，通用弱点枚举）类别来查看漏洞。CWE是一个分类系统，用于识别和分类软件设计和架构中的常见安全弱点或漏洞模式。

当想查看某一个漏洞详情页时可以点击蓝色字样的CVE ID， 以第一个**CVE-2024-4497**为例。



以下是界面中出现的字段的含义表述。

CVE漏洞库界面字段含义

基本信息

- **CVE ID**: 通用漏洞和暴露的唯一标识符
- **Summary**: 漏洞的简要描述
- **Vulnerability Details**: 详细说明漏洞的性质、触发条件和潜在影响
- **Identifier**: 分配给漏洞的其他标识符

时间戳

- **Last major update**: 最后一次重大更新的日期和时间
- **Published**: 漏洞首次公开发布的日期和时间
- **Last modified**: 最后一次修改记录的日期和时间
- **Status**: 漏洞当前的处理状态

CVSS（通用漏洞评分系统）

- **Base**: 基础风险评分
- **Impact**: 漏洞成功利用后造成的影响评分
- **Exploitability**: 漏洞被利用的难易程度评分
- **Vector**: 攻击途径（如网络、本地、物理等）
- **Complexity**: 成功攻击所需的复杂程度
- **Authentication**: 成功攻击前所需的认证级别
- **Confidentiality**: 对信息机密性的影响程度
- **Integrity**: 对系统完整性的影响程度
- **Availability**: 对系统可用性的影响程度

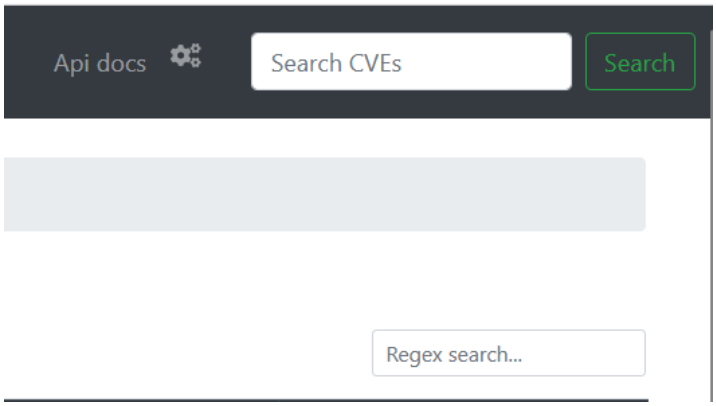
CVSS3（通用漏洞评分系统第3版）

- **Base**: 基础风险评分
- **Impact**: 影响评分
- **Exploitability**: 可利用性评分
- **Attack Complexity**: 成功攻击所需的技术复杂度
- **Attack vector**: 攻击者如何接触目标系统
- **Privileges Required**: 利用漏洞所需的权限级别

- **Score**: 评分变化状态
- **User Interaction**: 是否需要用户交互才能完成攻击
- **Confidentiality**: 信息机密性影响程度
- **Integrity**: 系统完整性影响程度
- **Availability**: 系统可用性影响程度

其他信息

- **EPSS**: 漏洞利用概率评分系统
- **EPSS %**: 漏洞被利用的概率百分比
- **References**: 与漏洞相关的参考资料链接
- **CAPEC**: 通用攻击模式枚举与分类
- **CWE**: 通用弱点枚举，漏洞的类型分类
- **Vulnerable Configurations**: 受该漏洞影响的系统配置
- **Source**: 漏洞信息的来源
- **Type**: 漏洞类型分类
- **Vector**: CVSS向量字符串，用于详细表示漏洞特征



Api docs: 是CVE库提供的一些API接口的使用场景，可以提供给用户编程使用

Search CVEs: 可以搜索CVE库中特定的cveID的详情信息

Regex search: 在当前页面可以使用正则表达式作为过滤器来过滤关键字