

权利要求书

- [权利要求 1] 一种NODE.JS组件漏洞检测方法，其特征在于，包括如下步骤：
从NODE.JS漏洞数据库中搜集第一基础漏洞信息；
解析package.json文件，获得NODE.JS组件的关键信息；
根据所述NODE.JS组件的关键信息，从所述第一基础漏洞信息提取第一目标漏洞信息。
- [权利要求 2] 如权利要求1所述的NODE.JS组件漏洞检测方法，其特征在于，所述根据所述NODE.JS组件的关键信息，从所述第一基础漏洞信息提取第一目标漏洞信息的步骤中，包括如下步骤：
根据关键信息的相关度，设定关键信息优先级；
获取CVE信息，以搜集CPE信息；
按照所述关键信息优先级，针对所述NODE.JS组件的关键信息与CPE信息进行匹配，生成第一目标漏洞信息。
- [权利要求 3] 如权利要求2所述的NODE.JS组件漏洞检测方法，其特征在于，所述根据所述NODE.JS组件的关键信息，从所述第一基础漏洞信息提取第一目标漏洞信息的步骤之后，包括如下步骤：
计算所述NODE.JS组件的sha1编码哈希值；
应用所述NODE.JS组件的sha1编码哈希值与所述NODE.JS第一目标漏洞信息进行匹配，生成第三目标漏洞信息。
- [权利要求 4] 如权利要求2所述的NODE.JS组件漏洞检测方法，其特征在于，所述针对所述NODE.JS组件的关键信息与CPE信息进行匹配，生成第一目标漏洞信息之后，还包括如下步骤：
从所述NODE.JS的关键信息中，提取NODE.JS组件名；
确认所述NODE.JS组件名与所述CPE信息一一对应。
- [权利要求 5] 如权利要求2所述的NODE.JS组件漏洞检测方法，其特征在于，所述生成第一目标漏洞信息的步骤之后，还包括如下步骤：
调用NODE.JS组件的接口，从所述package.json文件中，获取第二目标漏洞信息。

- [权利要求 6] 如权利要求5所述的NODE.JS组件漏洞检测方法，其特征在于，所述NODE.JS组件的关键信息包括NODE.JS组件的名称信息及NODE.JS组件的版本信息，所述获取第二目标漏洞信息的步骤之后，还包括如下步骤：
- 应用retirejs整理所述npm漏洞信息，获得第二基础漏洞信息；
- 根据所述NODE.JS组件的名称信息及NODE.JS组件的版本信息，与所述第二基础漏洞信息进行匹配，生成第三目标漏洞信息。
- [权利要求 7] 如权利要求6所述的NODE.JS组件漏洞检测方法，其特征在于，所述生成第三目标漏洞信息的步骤之后，还包括如下步骤：
- 定时下载更新的retirejs，以分析所述第三目标漏洞信息，生成第四目标漏洞信息。
- [权利要求 8] 如权利要求2所述的NODE.JS组件漏洞检测方法，其特征在于，所述根据所述NODE.JS组件的关键信息，从所述第一基础漏洞信息提取第一目标漏洞信息的步骤中，具体包括：
- 根据所述NODE.JS组件的关键信息，获取版本信息，产品名称及厂商信息；
- 分别应用所述版本信息，产品名称及厂商信息，与所述CPE信息进行匹配，获得匹配信息；
- 根据所述匹配信息，提取对应的CVE信息；
- 其中，所述CVE信息包括CVE编号。
- [权利要求 9] 如权利要求6所述的NODE.JS组件漏洞检测方法，其特征在于，所述第三目标漏洞信息包括漏洞信息、版本号信息、危险等级信息及CVE信息中的一种或多种。
- [权利要求 10] 一种NODE.JS组件漏洞检测系统，其特征在于，包括如下模块：
- 搜集模块，用于从NODE.JS漏洞数据库中搜集第一基础漏洞信息；
- 解析模块，用于解析package.json文件，获得NODE.JS组件的关键信息；
- 生成模块，用于根据所述NODE.JS组件的关键信息，从所述第一基础

漏洞信息提取第一目标漏洞信息。