

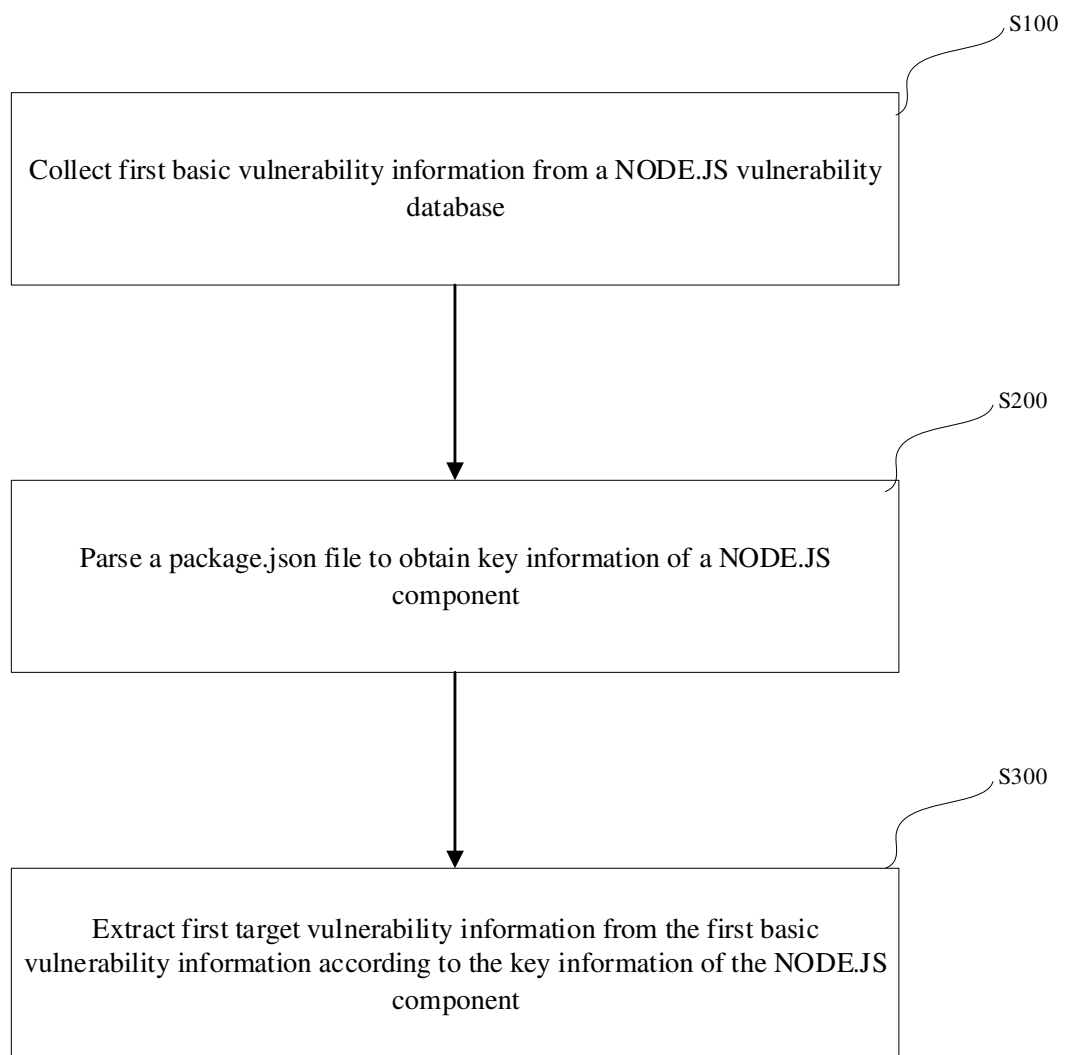


Fig. 1

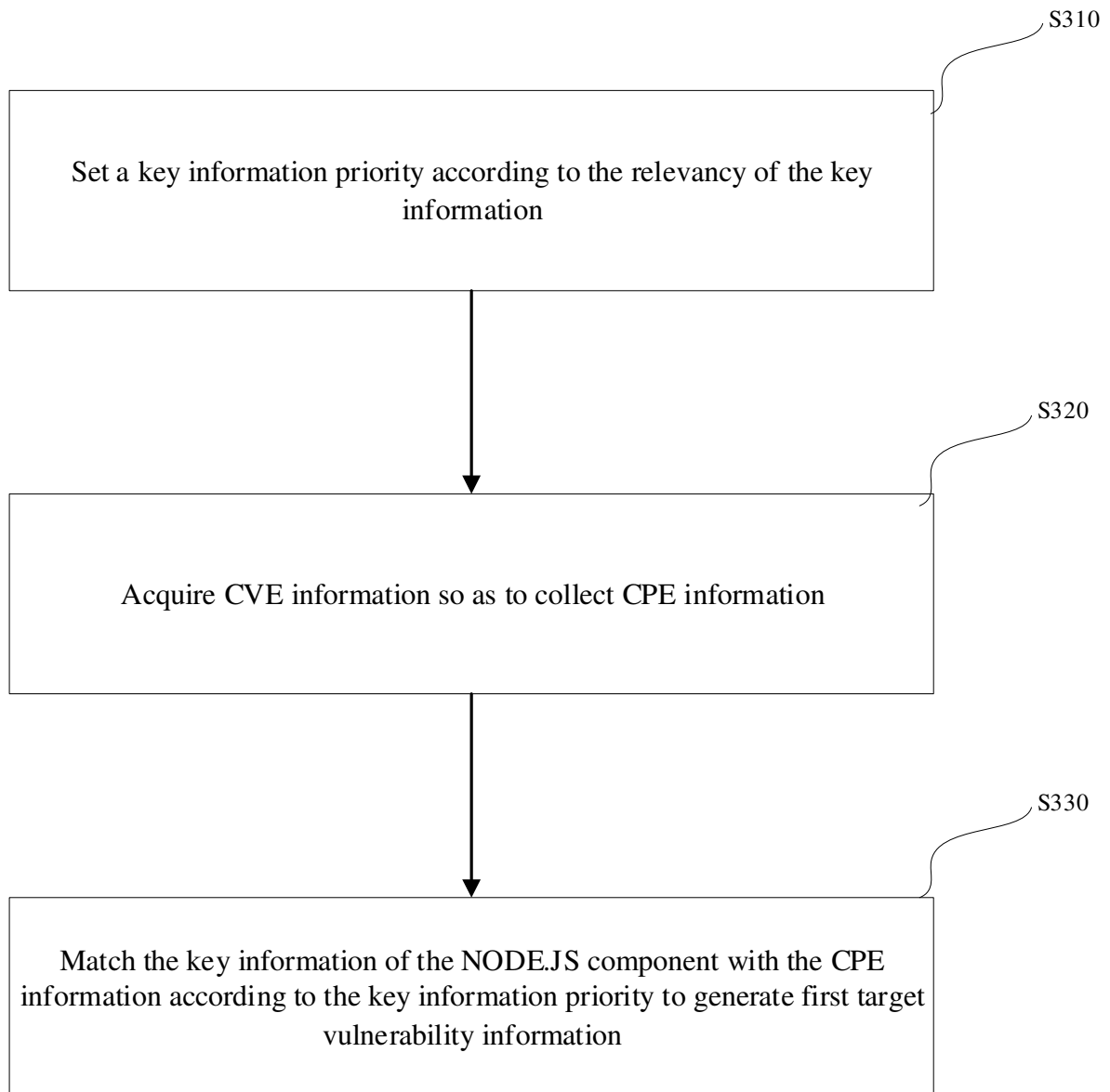


Fig. 2

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 [\(hide\)](#)

cpe:2.3:a:redhat:jboss_enterprise_application_platform:7.2.0:*:*:*:*:*

[Show Matching CPE\(s\)](#)

Running on/with

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*

[Show Matching CPE\(s\)](#)

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*

[Show Matching CPE\(s\)](#)

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*

[Show Matching CPE\(s\)](#)

Fig. 3



Fig. 4

Component name	sha1	cve number	cpe	vender	product	version	priority
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2014-1850	cpe:2.3.a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2014-3743	cpe:2.3.a:marked:marked:1.2:*****	marked	marked	1.2	High
js-yaml-2.0	e05ac5be948caacbc7e35003f746fa224e73c07	CVE-2013-4660	cpe:2.3.a:js-yaml:js-yaml:2.0:*****	js-yaml	js-yaml	2	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2019-004	cpe:2.3.a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	marked_content-injection					

Fig. 5

Component name	sha1	cve number	cpe	vender	product	version	priority
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2014-1850	cpe:2.3.a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High
js-yaml-2.0	e05ac5be948caacbc7e35003f746fa224e73c07	CVE-2013-4660	cpe:2.3.a:js-yaml:js-yaml:2.0:*****	js-yaml	js-yaml	2	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2019-004	cpe:2.3.a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	marked_content-injection					

Fig. 6

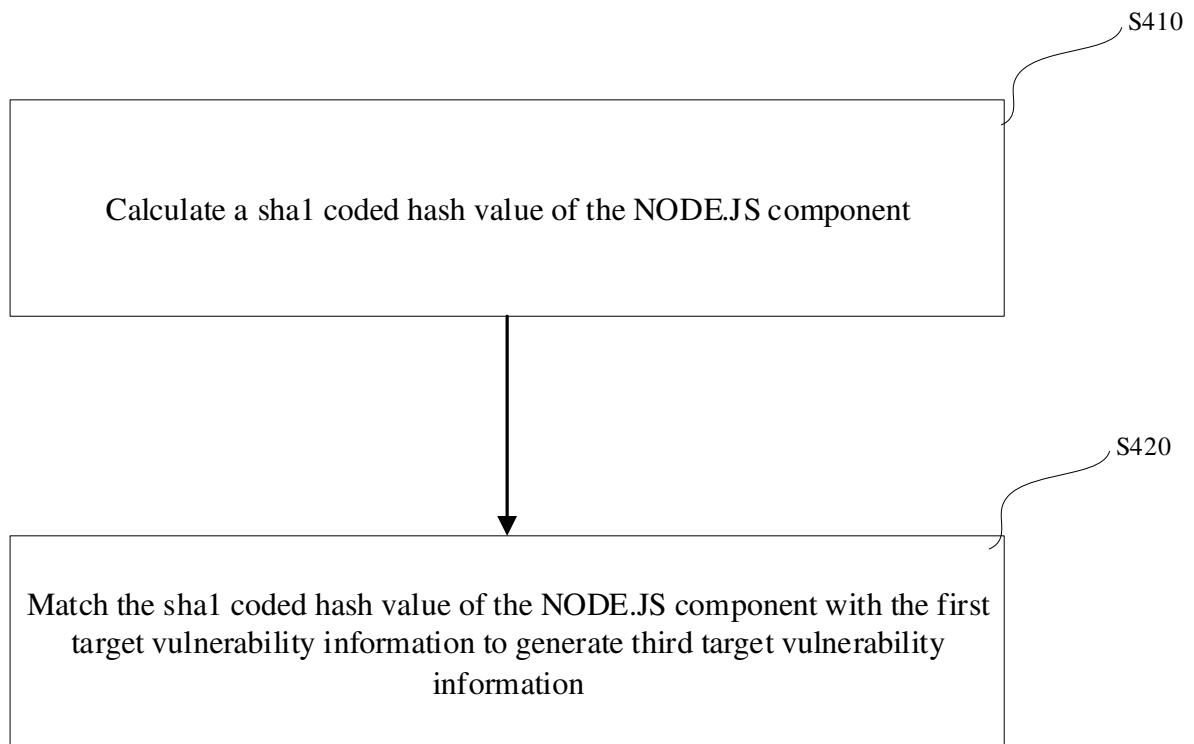


Fig. 7

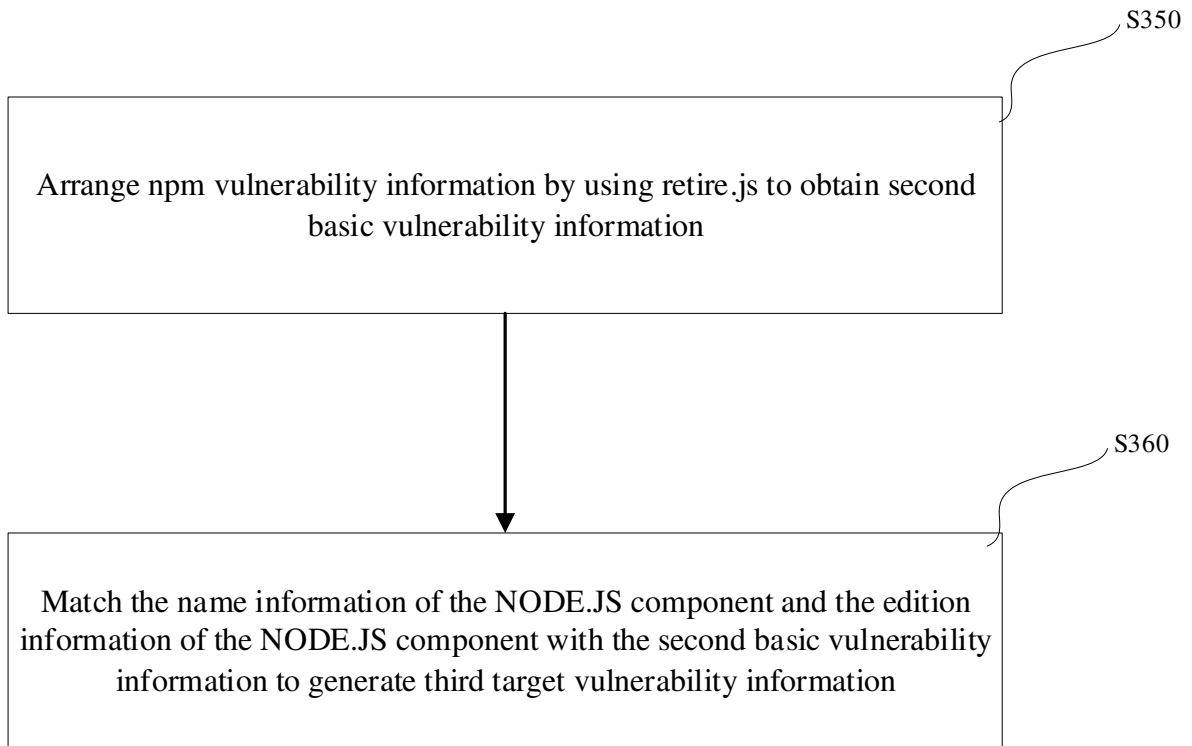


Fig. 8

```

"angular" : {
  "vulnerabilities" : [
    {
      "atOrAbove" : "1.5.0",
      "below" : "1.6.9",
      "severity": "low",
      "identifiers": {
        "summary": "XSS through SVG if enableSvg is set"
      },
      "info" : [ "https://github.com/angular/angular.js/blob/master/CHANGELOG.md#169-fiery-basilisk-2018-02-02",
        "https://vulnerabledoma.in/ngSanitize1.6.8_bypass.html" ]
    },
    {
      "atOrAbove" : "1.3.0",
      "below" : "1.5.0-rc2",
      "severity": "medium",
      "identifiers": {
        "summary": "The attribute usemap can be used as a security exploit"
      },
      "info" : [ "https://github.com/angular/angular.js/blob/master/CHANGELOG.md#1230-patronal-resurrection-2016-07-21" ]
    }
  ],

```

Fig. 9

Component name	sha1	cve number	cpe	vender	product	version	priority
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2014-1850	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High
js-yaml-2.0	e05ac5be948caacbc7e35003f746fa224e73c07	CVE-2013-4660	cpe:2.3:a:js-yaml:js-yaml:2.0:*****	js-yaml	js-yaml	2	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2019-004	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	marked_content_injection					
marked-0.3.5	7eba06fed3f032493f3e55b6c5b323f7737c78b0	CVE-2020-001	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	High

Fig. 10

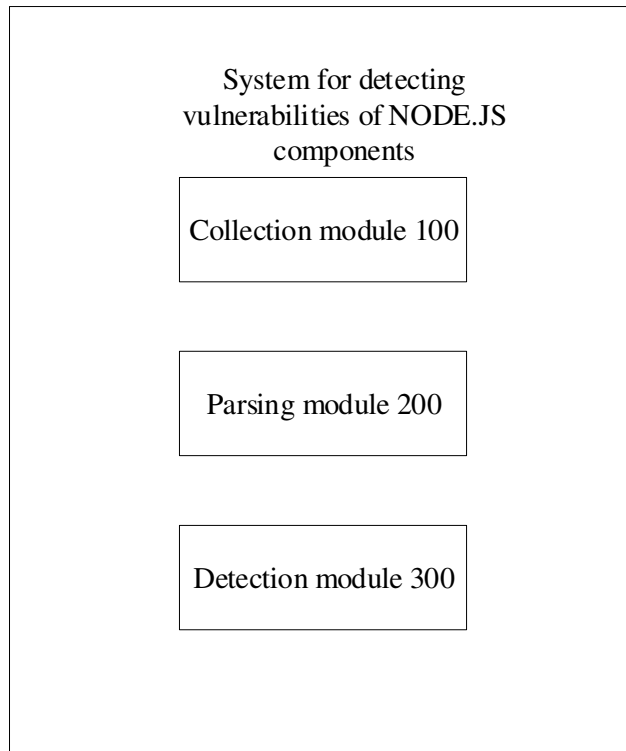


Fig. 11