

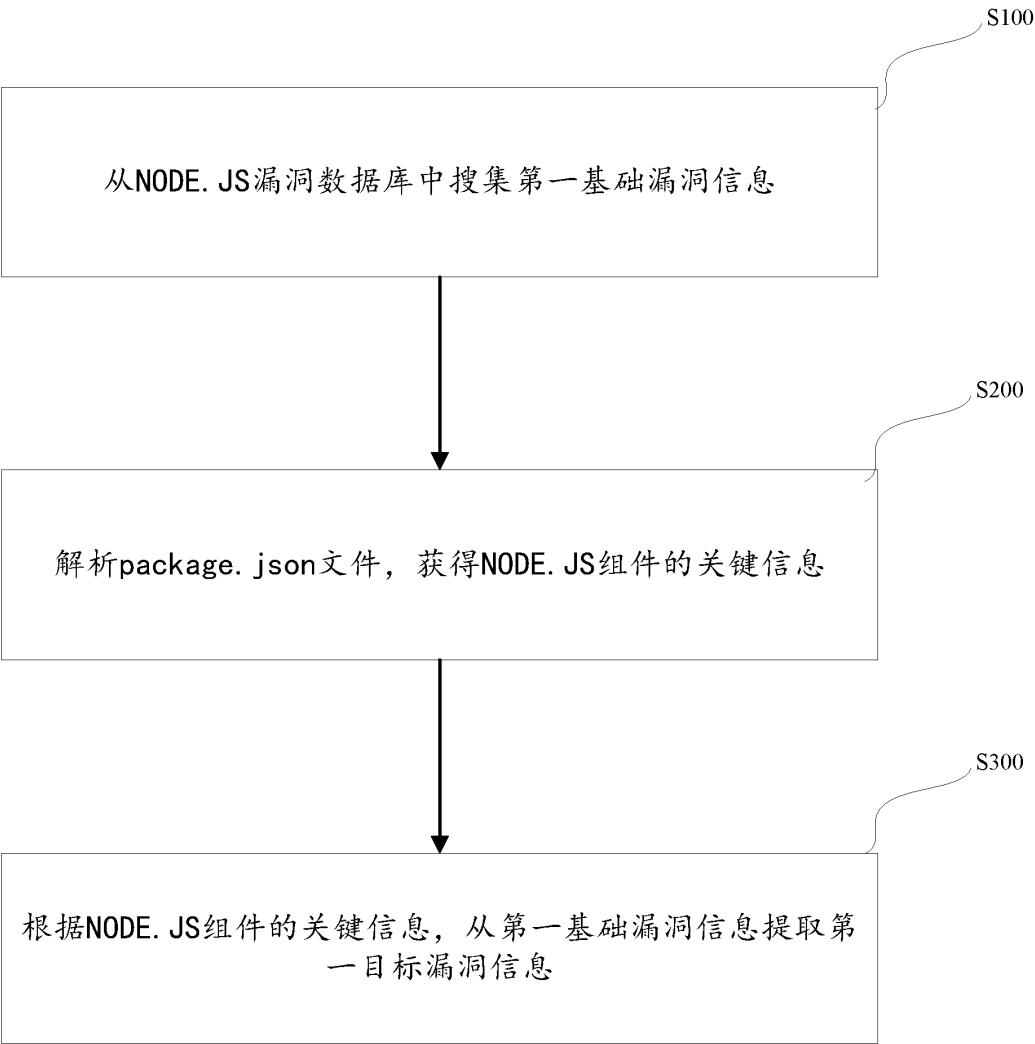


图 1

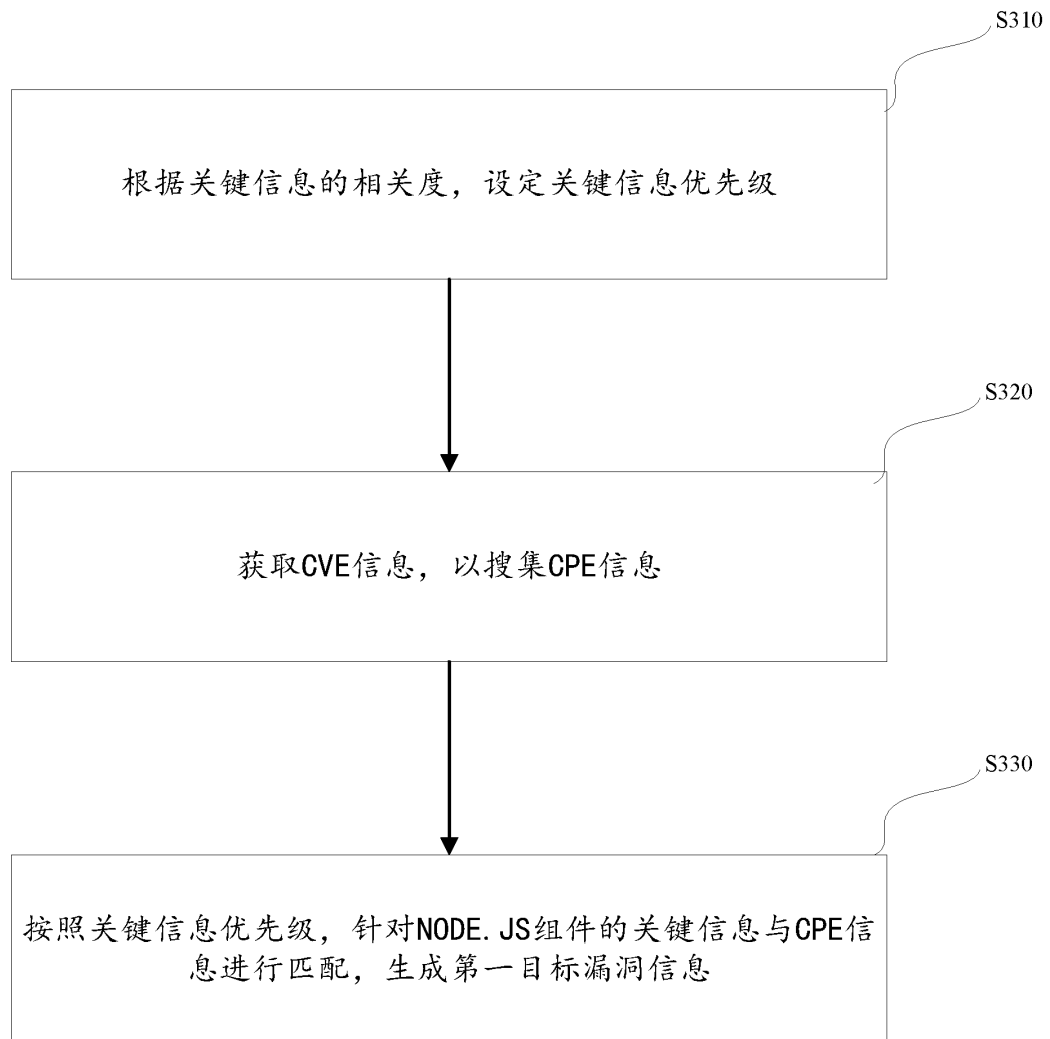


图 2

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) ▼

图 3

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

Show Matching CPE(s) ▼

图 4

组件名	sha1	cve编号	cpe	vendor	product	version	priority
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	CVE-2014-1830	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	高
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	CVE-2014-3743	cpe:2.3:a:marked:marked:1.2:*****	marked	marked	1.2	高
js-yaml:2.0	e05a55e948caacbb7e35030746fa224e73cd7	CVE-2013-4660	cpe:2.3:a:js-yaml:js-yaml:2.0:*****	js-yaml	js-yaml	2.0	高
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	CVE-2019-004	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	高
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	marked:content-injection					

图 5

组件名	sha1	cve编号	cpe	vendor	product	version	priority
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	CVE-2014-1830	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	高
js-yaml:2.0	e05a55e948caacbb7e35030746fa224e73cd7	CVE-2013-4660	cpe:2.3:a:js-yaml:js-yaml:2.0:*****	js-yaml	js-yaml	2.0	高
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	CVE-2019-004	cpe:2.3:a:marked:marked:0.3.5:*****	marked	marked	0.3.5	高
marked-0.3.5	7eba08fed30324930e5b6c5b323f7737c78b0	marked:content-injection					

图 6

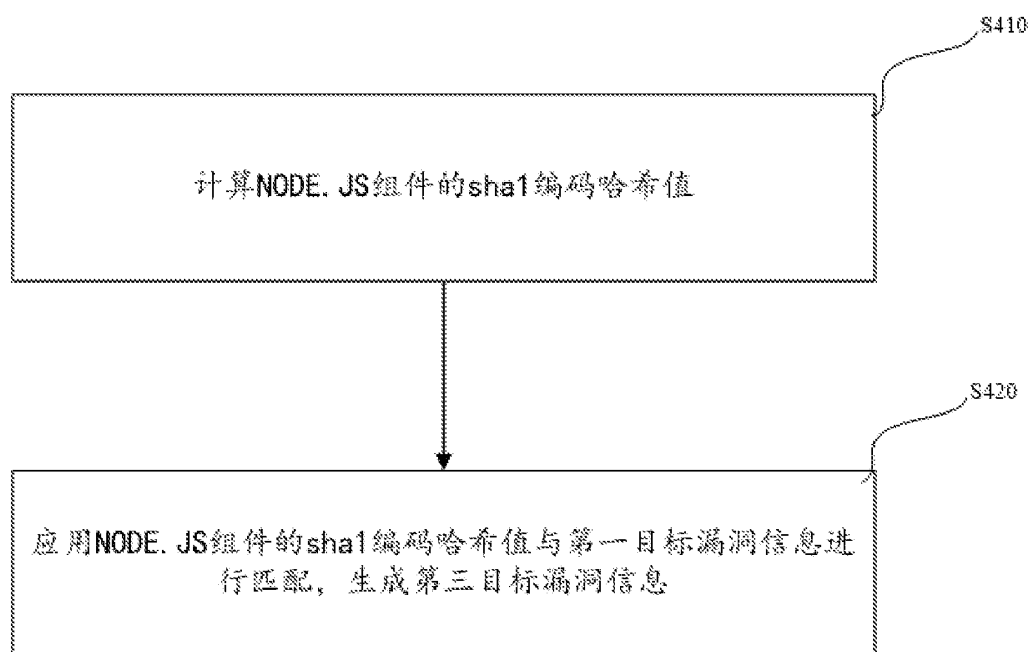


图 7

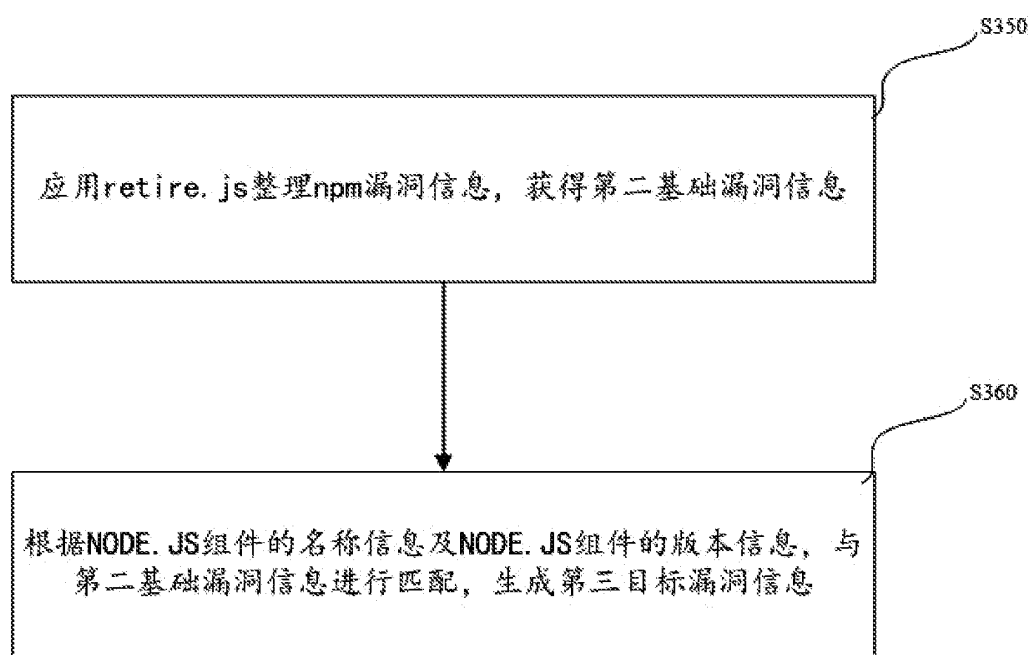


图 8

```
"angular": {}
"vulnerabilities": [
{
  "atOrAbove": "1.5.8",
  "below": "1.6.0",
  "severity": "low",
  "identifiers": {
    "summary": "XSS through SVG if enableSvg is set"
  },
  "info": [
    "https://github.com/angular/angular.js/blob/master/CHANGELOG.md#160-fiery-basilisk-2018-02-02",
    "https://vulnerabilities.in/ngSanitize1.6.8_bypass.html" ]
  },
{
  "atOrAbove": "1.1.8",
  "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#1238-patronal-resurrection-2015-07-21" ]
  },
]
```

图 9

包名称	URL	CVE编号	CWE	verified	exploited	known	score
marked 0.15	7efac5b6d58c7e458303746e224e73e07	CVE-2014-1850	cpp.13a marked marked 0.15	marked	marked	0.15	35
js-vanilla-2.0	7efac5b6d58c7e458303746e224e73e07	CVE-2013-4850	cpp.13a js-vanilla-vanilla 2.0	marked	marked	0.15	35
marked 0.15	7efac5b6d58c7e458303746e224e73e07	CVE-2013-3524	cpp.13a marked marked 0.15	marked	marked	0.15	35
marked 0.15	7efac5b6d58c7e458303746e224e73e07	marked content function					
marked 0.15	7efac5b6d58c7e458303746e224e73e07	CVE-2013-3521	cpp.13a marked marked 0.15	marked	marked	0.15	35

图 10



图 11