

**How to read the report** | **Suppressing false positives** | **Getting Help: google group** | **github issues**

## Project: noruby_dependency_check

Scan Information (show all):

- *dependency-check version*: 1.4.5
- *Report Generated On*: Mar 11, 2017 at 06:27:53 +05:30
- *Dependencies Scanned*: 10 (10 unique)
- *Vulnerable Dependencies*: 1
- *Vulnerabilities Found*: 4
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing All Dependencies (click to show less)

| Dependency | CPE | GAV | Highest Severity | CVE Count | CPE Confidence | Evidence Count |
|---|---|---|---|---|---|---|
| rubypluginhelp.jar | | | | 0 | | 4 |
| rubypluginhelp_mac.jar | | | | 0 | | 4 |
| bytelist-1.0.2.jar | | | | 0 | | 5 |
| jcodings-1.0.10.jar | | org.jruby.jcodings:jcodings:1.0.10 | | 0 | | 11 |
| joda-time-2.3.jar | | joda-time:joda-time:2.3 | | 0 | | 22 |
| joni-2.0.0.jar | | org.jruby.joni:joni:2.0.0 | | 0 | | 11 |
| jvyamlb-0.2.5.jar | | | | 0 | | 3 |
| kxml2-2.3.0.jar | cpe:/a:google:android:2.3.0 | net.sf.kxml:kxml2:2.3.0 | High | 4 | LOW | 15 |
| ruby.jar | | | | 0 | | 4 |
| snakeyaml-1.13.jar | | org.yaml:snakeyaml:1.13 | | 0 | | 15 |

## Dependencies

### rubypluginhelp.jar

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/help/rubypluginhelp.jar
**MD5:** da6961c3383d8b92a814c339af949217
**SHA1:** 8af7793ec75c8e7e33fc7a6866aebc771295895f

**Evidence**

**Identifiers**

- **None**

### rubypluginhelp_mac.jar

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/help/rubypluginhelp_mac.jar
**MD5:** f50792d887c72341af60085a861ab0a0
**SHA1:** e8605bdd13c846f436e36a2690dc6ebbad9ab4e5

**Evidence**

**Identifiers**

- **None**

### bytelist-1.0.2.jar

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/bytelist-1.0.2.jar
**MD5:** 466d93524df204379ff9e4ef6ea92795
**SHA1:** 4bf5037dedacbd07f8e6fbc6a3c0da7295650a36

**Evidence**

**Identifiers**

- **None**

### jcodings-1.0.10.jar

**Description:** Byte based encoding support library for java

**License:**

```
MIT License: http://www.opensource.org/licenses/mit-license.php
```

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/jcodings-1.0.10.jar
**MD5:** 7a91c91d90b3182403ca5751453f2ad2
**SHA1:** 6ed6198bcc291ae4375da82992d956f765d98eec

**Evidence**

**Identifiers**

- **maven:** org.jruby.jcodings:jcodings:1.0.10 *Confidence*:HIGHEST

### joda-time-2.3.jar

**Description:** Date and time library to replace JDK date handling

**License:**

```
Apache 2: http://www.apache.org/licenses/LICENSE-2.0.txt
```

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/joda-time-2.3.jar
**MD5:** ff85fe8f3ab26b36092475a95f43fb7e
**SHA1:** 56498efd17752898cfcc3868c1b6211a07b12b8f

**Evidence**

**Identifiers**

- **maven:** joda-time:joda-time:2.3 *Confidence*:HIGHEST

### joni-2.0.0.jar

**Description:** Java port of Oniguruma: http://www.geocities.jp/kosako3/oniguruma that uses byte arrays directly instead of java Strings and chars

**License:**

```
MIT License: http://www.opensource.org/licenses/mit-license.php
```

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/joni-2.0.0.jar
**MD5:** b61a599a0b7b2f21fab362e923ad0605
**SHA1:** 5f0e5b509ada9cd568c58be6c6d048d82507cc0b

**Evidence**

**Identifiers**

- **maven:** org.jruby.joni:joni:2.0.0 *Confidence*:HIGHEST

### jvyamlb-0.2.5.jar

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/jvyamlb-0.2.5.jar
**MD5:** 9e7de2e86fcd1e57ddbea0678e9f062f
**SHA1:** c74891652513858b41081b8481a616c6a0a519fe

**Evidence**

**Identifiers**

- **None**

### kxml2-2.3.0.jar

**Description:** A library jar that provides APIs for Applications written for the Google Android Platform.

**License:**

```
Apache 2.0: http://www.apache.org/licenses/LICENSE-2.0
```

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/kxml2-2.3.0.jar

**MD5:** 04a03b3a4f1ef0e3fda28bf1792e2ee7
**SHA1:** ccbc77a5fd907ef863c29f3596c6f54ffa4e9442

**Evidence**

**Identifiers**

- **cpe:** cpe:/a:google:android:2.3.0 *Confidence*:LOW suppress
- **maven:** net.sf.kxml:kxml2:2.3.0 *Confidence*:HIGHEST
- **maven:** org.robolectric:android-kxml2:4.1.2_r1_rc *Confidence*:HIGHEST

**Published Vulnerabilities**

**CVE-2016-5696** suppress

Severity: Medium
CVSS Score: 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)
CWE: CWE-200 Information Exposure

net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.

- BID - 91704
- CONFIRM - http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=75ff39ccc1bd5d3c455b6822ab09e533c551f758
- CONFIRM - http://source.android.com/security/bulletin/2016-10-01.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
- CONFIRM - https://bto.bluecoat.com/security-advisory/sa131
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1354708
- CONFIRM - https://github.com/torvalds/linux/commit/75ff39ccc1bd5d3c455b6822ab09e533c551f758
- CONFIRM - https://kc.mcafee.com/corporate/index?page=content&id=SB10167
- MISC - http://www.prnewswire.com/news-releases/mitnick-attack-reappears-at-geekpwn-macau-contest-300270779.html
- MISC - https://github.com/Gnoxter/mountain_goat
- MISC - https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_cao.pdf
- MLIST - [oss-security] 20160712 Re: CVE-2016-5389: linux kernel - challange ack information leak.
- REDHAT - RHSA-2016:1631
- REDHAT - RHSA-2016:1632
- REDHAT - RHSA-2016:1633
- REDHAT - RHSA-2016:1657
- REDHAT - RHSA-2016:1664
- REDHAT - RHSA-2016:1814
- REDHAT - RHSA-2016:1815
- SECTRACK - 1036625
- UBUNTU - USN-3070-1
- UBUNTU - USN-3070-2
- UBUNTU - USN-3070-3
- UBUNTU - USN-3070-4
- UBUNTU - USN-3071-1
- UBUNTU - USN-3071-2
- UBUNTU - USN-3072-1
- UBUNTU - USN-3072-2

Vulnerable Software & Versions: (show all)

- cpe:/a:google:android:7.0 and all previous versions
- ...

**CVE-2014-6060** suppress

Severity: Low
CVSS Score: 3.3 (AV:A/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399 Resource Management Errors

The get_option function in dhcpcd 4.0.0 through 6.x before 6.4.3 allows remote DHCP servers to cause a denial of service by resetting the DHO_OPTIONSOVERLOADED option in the (1) bootfile or (2) servername section, which triggers the option to be processed again.

- BID - 68970
- CONFIRM - http://advisories.mageia.org/MGASA-2014-0334.html
- CONFIRM - http://roy.marples.name/projects/dhcpcd/ci/1d2b93aa5ce25a8a710082fe2d36a6bf7f5794d5?sbs=0
- CONFIRM - http://source.android.com/security/bulletin/2016-04-02.html
- MANDRIVA - MDVSA-2014:171
- MLIST - [oss-security] 20140730 CVE Request: dhcpcd DoS attack
- MLIST - [oss-security] 20140901 CVE Request: dhcpcd DoS attack
- SLACKWARE - SSA:2014-213-02

Vulnerable Software & Versions: (show all)

- cpe:/a:google:android:4.4.3 and all previous versions
- ...

**CVE-2014-1939** suppress

Severity: High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-94 Improper Control of Generation of Code ('Code Injection')

java/android/webkit/BrowserFrame.java in Android before 4.4 uses the addJavascriptInterface API in conjunction with creating an object of the SearchBoxImpl class, which allows attackers to execute arbitrary Java code by leveraging access to the searchBoxJavaBridge_ interface at certain Android API levels.

- CONFIRM - http://blog.chromium.org/2013/11/introducing-chromium-powered-android.html
- CONFIRM - https://support.lenovo.com/us/en/product_security/len_6421
- MLIST - [oss-security] 20140210 CVE-2014-1939 searchBoxJavaBridge_ in Android Jelly Bean

Vulnerable Software & Versions: (show all)

- cpe:/a:google:android:4.3.1 and all previous versions
- ...

**CVE-2013-7372** suppress

Severity: Medium
CVSS Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-310 Cryptographic Issues

The engineNextBytes function in classlib/modules/security/src/main/java/common/org/apache/harmony/security/provider/crypto/SHA1PRNG_SecureRandomImpl.java in the SecureRandom implementation in Apache Harmony through 6.0M3, as used in the Java Cryptography Architecture (JCA) in Android before 4.4 and other products, when no seed is provided by the user, uses an incorrect offset value, which makes it easier for attackers to defeat cryptographic protection mechanisms by leveraging the resulting PRNG predictability, as exploited in the wild against Bitcoin wallet applications in August 2013.

- CONFIRM - http://android-developers.blogspot.com.au/2013/08/some-securerandom-thoughts.html
- CONFIRM - https://android.googlesource.com/platform/libcore/+/kitkat-release/luni/src/main/java/org/apache/harmony/security/provider/crypto/SHA1PRNG_SecureRandomImpl.java
- MISC - http://www.nds.rub.de/media/nds/veroeffentlichungen/2013/03/25/paper_2.pdf
- MISC - https://bitcoin.org/en/alert/2013-08-11-android

Vulnerable Software & Versions: (show all)

- cpe:/a:google:android:4.3.1 and all previous versions
- ...

### ruby.jar

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/ruby.jar
**MD5:** b490ee3259d575cca19e51fafc4a487d
**SHA1:** eacfd5580f8a851aed8657e0fcdfda14269e8eba

**Evidence**

**Identifiers**

- **None**

### snakeyaml-1.13.jar

**Description:** YAML 1.1 parser and emitter for Java

**License:**

```
Apache License Version 2.0: LICENSE.txt
```

**File Path:** /home/caesar/caesarcypher.info/OWASP_Dependency_Checker/Plugins/ruby/lib/snakeyaml-1.13.jar
**MD5:** 88e239ab48632e2eab576ee86f56c47e
**SHA1:** 73cbb494a912866c4c831a178c3a2a9169f4eaad

**Evidence**

**Identifiers**

- **maven:** org.yaml:snakeyaml:1.13 *Confidence*:HIGHEST

This report contains data retrieved from the National Vulnerability Database.