



CVE-2013-1624

Published on: 02/08/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:32 PM UTC

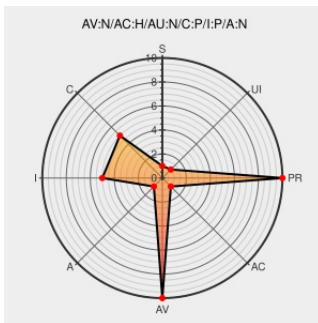
CVE-2013-1624

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Legion-of-the-bouncy-castle-c-cryptography-api](#) from [Bouncycastle](#) contain the following vulnerability:

The TLS implementation in the Bouncy Castle Java library before 1.48 and C# library before 1.8 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

CVE-2013-1624 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0371
Security Advisory SA57716 - Red Hat update for Red Hat JBoss BPM Suite - Secunia	web.archive.org text/html	SECUNIA 57716
Security Advisory SA57719 - Red Hat update for Red Hat JBoss BRMS - Secunia	web.archive.org text/html	SECUNIA 57719
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0372

oss-security - Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations

[openwall.com
text/html](https://openwall.com/text/html)

 [MLIST \[oss-security\] 20130205 Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations](#)

[www.isg.rhul.ac.uk
application/pdf](http://www.isg.rhul.ac.uk/application/pdf)

 [MISC www.isg.rhul.ac.uk/tls/TLStiming.pdf](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	0.0	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.0	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.1	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.2	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.3	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.4	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.5	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.6.1	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.7	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	0.0	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.0	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.1	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.2	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.3	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.4	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.5	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.6.1	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.7	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	0.0	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.0	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.1	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.2	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.3	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-c-cryptography-api	1.4	All	All	All

[illegible]

[illegible]

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.6.1:*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.7:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c\#-cryptography-api:0.0:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c\#-cryptography-api:1.0:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.1:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.2.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#\cryptography-api:1.3.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c\#-cryptography-api:1.4:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.5:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.6.1:***:***:***:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.7:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c/#-cryptography-api:0.0:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c\#-cryptography-api:1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c/#-cryptography-api:1.1:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c\#-cryptography-api:1.2:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.3:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.4.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c\#-cryptography-api:1.5:::*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-c#-cryptography-api:1.7:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.01::*:.*:*.*.*.*
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.02:::*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.03:***:***:***:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.04:***:***:***:***:***:***:***
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.05:***:***:***:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.06:***:***:***:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.07:***:***:***:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.08:*.***.***.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.09:*.***.***.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.10:*:*:*:*:*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.11.*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.12:*.**:*.**:*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.13:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.14:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.15:*:*:*:*:*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.16:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.17:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.18:*.**:*.**:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.19:*.**:*.**:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.20:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.21:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.22:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.23:*.***.***.*:
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.24:*:*:*:*:*.*

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.25:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.26:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.27:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.28:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.29:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.30:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.31.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.32:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.33:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.34:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.35:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.36:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.37:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.38:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.39:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.40:*:*:*:*:*:
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.41:*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.42:*:*:*:*:*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.43:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.44:*:*:*:*:*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.45:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.46:*:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.47:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.01:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.02:*.***.***.*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.03:*.**:*.**:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.04:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.05:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.06:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.07:*:*:*:*:*.*
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.08:*:*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.09:*.**:*.**:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.10:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.11:*.*:*.*:*.:
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.12:*:*:*:*:*:*

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.13:*.*:*.*:*.:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.14:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.15:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.16:*.*:*.*:.*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.17:*.***.***.*:
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.18:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:lejon-of-the-bouncy-castle-java-cryptography-api:1.19:***:***:***:
```

Topographic location of the study area and topography map.

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.20:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.21:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.22:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.23:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.24:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.25:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.26:*:*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.27:*:*:*:*:*:
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.28:*:*:*:*:*:*

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.29:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.30:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.31:::*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.32:*.**:*.**:.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.33:::*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.34:::*:*:*:*:*
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.35:::*:*:*:*:*

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.36:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.37:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.38:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.39:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.40:::*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.41:::*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.42:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.43:::*:*:*:*:*

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.44:*:*:*:*:*:*:

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.45:*:*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.46:***:***:***:
```

cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.47:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)