



CVE-2007-6721

Published on: 03/29/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:39 PM UTC

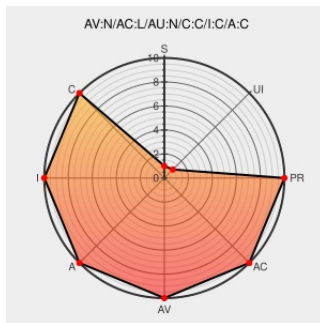
CVE-2007-6721

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Bouncy-castle-crypto-package](#) from [Bouncycastle](#) contain the following vulnerability:

The Legion of the Bouncy Castle Java Cryptography API before release 1.38, as used in Crypto Provider Package before 1.36, has unknown impact and remote attack vectors related to "a Bleichenbacher vulnerability in simple RSA CMS signatures without signed attributes."

CVE-2007-6721 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

[www.osvdb.org](#)

OSVDB 50358

Inactive Link Not Archived

bouncycastle.org :: dev-crypto :: [dev-crypto]
Bouncy Castle Crypto Provider Package
version 1.36 now available

[Patch](#)
[Vendor Advisory](#)
[www.bouncycastle.org](#)
[text/html](#)

MLIST [dev-crypto] 20071109 Bouncy Castle Crypto
Provider Package version 1.36 now available

bouncycastle.org

[www.bouncycastle.org](#)
[text/html](#)

CONFIRM [www.bouncycastle.org/releasesnotes.html](#)

All releases of Legion of the Bouncy Castle
Java Cryptography API – Freecode

[freshmeat.net](#)
[text/html](#)

CONFIRM
[freshmeat.net/projects/bouncycastlecryptoapi/releases/265580](#)

No Description Provided	www.osvdb.org	 OSVDB 50359
	Inactive Link	Not Archived
No Description Provided	www.osvdb.org	 OSVDB 50360
	Inactive Link	Not Archived
The Legion of the Bouncy Castle C# Cryptography APIs	Patch Vendor Advisory www.bouncycastle.org text/html	 CONFIRM www.bouncycastle.org/csharp/

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.

Related QID Numbers

995463 Java (Maven) Security Update for bouncycastle:bcprov-jdk14 (GHSA-m26p-m559-g5j5)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Bouncy-castle-crypto-package	1.0	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.01	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.02	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.03	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.04	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.05	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.06	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.07	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.08	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.09	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.11	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.12	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.13	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.14	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.15	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.16	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.17	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.18	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.19	All	All	All
Application	Bouncycastle	Bouncy-castle-crypto-package	1.20	All	All	All

[illegible]

[illegible]

[illegible]

Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.22	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.23	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.24	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.25	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.26	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.27	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.28	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.29	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.30	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.31	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.32	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.33	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.34	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.35	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.36	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	All	All	All	All

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.0:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.01:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.02:*.:.:.:.:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.03:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.04:*:*:*:*.*.*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.05:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.06.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.07:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.08:*.***.***:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.09:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.11:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.12::*:*:*:*:*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.13:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.14.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.15:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.16::*:.*:*.*.*.*.*.*
```

cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.17:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.18:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.19:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.20:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.21:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.22:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.23:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.24:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.25:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.26:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.27:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.28:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.29:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.3.1:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.30:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.32:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.33:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.34:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.0:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.01:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.02:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.03:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.04:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.05:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.06:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.07:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.08:*****:
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.09:*****:

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.11:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.12:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.13:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.14.*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.15:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.16:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.17:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.18:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.19:::*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.20:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.21:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.22:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.23:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.24:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.25:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.26:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.27:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.28:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.29:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.3.1:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.30:*:*:*:*:*.*
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.32:*:*:*:*:*:
```

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.33.*:*:*:*:*.*
```

cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.34:*:*:*:*:*:

```
cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:*:*:*:*:*:*.*
```

```
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:*****.*.*.*
```


[illegible]

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:1.01:::*:*:*:*:*:
```

```
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:::*:*:*:*:*
```

```
one:2 2:a:hounycastle:logon of the hounyc castle iava cryptography one:1 25:***.***.***.
```

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:1.26:*****:
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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)