



# CVE-2016-1000346

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2016-1000346
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-04 21:29:00 UTC
<b>Updated</b>	2020-10-20 22:15:00 UTC
<b>Description</b>	In the Bouncy Castle JCE Provider version 1.55 and earlier the other party DH public key is not fully validated. This can cau

## Risk And Classification

**Problem Types:** CWE-320

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Bouncycastle</a>	<a href="#">Legion-of-the-bouncy-castle-java-cryptography-api</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All

## References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	
Oracle Critical Patch Update Advisory - October 2020	MISC	<a href="#">www.oracle.com</a>	
June 2018 Bouncy Castle Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	
Added TLS validation check for DH keys · bcgit/bc-java@1127131 · GitHub	CONFIRM	<a href="#">github.com</a>	Patch, Third Pa
[SECURITY] [DLA 1418-1] bouncycastle security update	MLIST	<a href="#">lists.debian.org</a>	Third Party Adv
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	
USN-3727-1: Bouncy Castle vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analy

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

981105 Java (maven) Security Update for org.bouncycastle:bcprov-jdk15 (GHSA-fjqm-246c-mwqg)

© [CVE.report](#) 2026 |

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](#)