



CVE-2016-1000343

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-1000343
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-04 13:29:00 UTC
Updated	2023-11-07 02:29:00 UTC
Description	In the Bouncy Castle JCE Provider version 1.55 and earlier the DSA key pair generator generates a weak private key if use

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	
Pony Mail!		lists.apache.org	
updated default DSA parameters to follow 186-4 · bcgit/bc-java@50a5306 · GitHub	CONFIRM	github.com	Patch, Third Pa
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
June 2018 Bouncy Castle Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] [DLA 1418-1] bouncycastle security update	MLIST	lists.debian.org	Third Party Adv
Pony Mail!	MLIST	lists.apache.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
USN-3727-1: Bouncy Castle vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980871 Java (maven) Security Update for org.bouncycastle:bcprov-jdk15 (GHSA-rrvx-pwf8-p59p)

© [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](#)