CVE-2016-1000343

MITRE | NVD | CVE.ORG | Print: PDF

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-crytography-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, analy

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)