CVE-2016-1000338

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-1000338
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-01 20:29:00 UTC
Updated	2023-11-07 02:29:00 UTC
Description	In Bouncy Castle JCE Provider version 1.55 and earlier the DSA does not fully validate ASN.1 encoding of signature on ver

Risk And Classification

Problem Types: CWE-347

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

References

Reference	Source	Link	Tags
CVE-2016-1000338 Bouncy Castle Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
[SECURITY] [DLA 1418-1] bouncycastle security update	MLIST	lists.debian.org	Mailing
Pony Mail!	MLIST	lists.apache.org	
added length check for sequence in DSA signatures · bcgit/bc-java@b0c3ce9 · GitHub	CONFIRM	github.com	Patch, T
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	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981307 Java (maven) Security Update for org.bouncycastle:bcprov-jdk15 (GHSA-4vhj-98r6-424h)