CVE-2017-13098

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-13098
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-13 01:29:00 UTC
Updated	2020-10-20 22:15:00 UTC
Description	BouncyCastle TLS prior to version 1.0.3, when configured to use the JCE (Java Cryptography Extension) for cryptographic

Risk And Classification

Problem Types: CWE-203

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
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-crytography-api	All	All	All	All

References

Reference	So
Debian -- Security Information -- DSA-4072-1 bouncycastle	DE
[security-announce] openSUSE-SU-2020:0607-1: moderate: Security update f	SU
Oracle Critical Patch Update Advisory - October 2020	MI
CVE-2017-13098 Bouncy Castle TLS Vulnerability in NetApp Products | NetApp Product Security	CC
The ROBOT Attack - Return of Bleichenbacher's Oracle Threat	MI
VU#144389 - TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding	CE
Bouncy Castle CVE-2017-13098 Information Disclosure Vulnerability	BI
Confirm size of decrypted PMS before using · bcgit/bc-java@a00b684 · GitHub	CC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report