



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

References

Reference	Source
Debian -- Security Information -- DSA-4072-1 bouncycastle	DEBIAN
[security-announce] openSUSE-SU-2020:0607-1: moderate: Security update f	SUSE
Oracle Critical Patch Update Advisory - October 2020	MISC
CVE-2017-13098 Bouncy Castle TLS Vulnerability in NetApp Products NetApp Product Security	CC
The ROBOT Attack - Return of Bleichenbacher's Oracle Threat	MISC
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	BID
Confirm size of decrypted PMS before using · bcgit/bc-java@a00b684 · GitHub	CC
CVE Program record	CV
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#)