



CVE-2015-7824

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-7824
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-10 15:59:00 UTC
Updated	2017-04-15 00:42:00 UTC
Description	botan 1.11.x before 1.11.22 makes it easier for remote attackers to decrypt TLS ciphertext data via a padding-oracle attack

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Botan Project	Botan	All	All	All	All

References

Reference	Source	Link	Tags
Security — Botan	CONFIRM	botan.randombit.net	Vendor Advisory
1311613 – (CVE-2015-7824) CVE-2015-7824 botan: padding oracle attack on TLS	CONFIRM	bugzilla.redhat.com	Issue Tracking, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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