CVE-2015-2141

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-2141
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-01 14:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The InvertibleRWFunction::CalculateInverse function in rw.cpp in libcrypt++ 5.6.2 does not properly blind private key operat

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cryptopp	Crypto Library	5.6.2	All	All	All
Application	Cryptopp	Crypto Library	5.6.2	All	All	All
Application	Cryptopp	Crypto Library	5.6.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

References

Reference	Source	Link
Crypto++ CVE-2015-2141 Information Disclosure Vulnerability	BID	www.securit
openSUSE-SU-2015:1271-1: moderate: Security update for libcryptopp	SUSE	lists.opensu
Crypto++ / Code / Commit [r542]	CONFIRM	sourceforge
Debian -- Security Information -- DSA-3296-1 libcrypto++	DEBIAN	www.debian
Fix for CVE-2015-2141. Thanks to Evgeny Sidorov for reporting. Squari… · weidai11/cryptopp@9425e16 · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

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