CVE-2016-6129

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-6129
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-13 18:59:00 UTC
Updated	2017-03-13 15:24:00 UTC
Description	The rsa_verify_hash_ex function in rsa_verify_hash.c in LibTomCrypt, as used in OP-TEE before 2.2.0, does not validate th

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libtom	Libtomcrypt	All	All	All	All
Operating System	Op-tee	Op-tee Os	All	All	All	All

References

Reference	Source	Link	Tag
404 page not found! - OP-TEE	CONFIRM	www.op-tee.org	Ver
rsa_verify_hash: fix possible bleichenbacher signature attack · libtom/libtomcrypt@5eb9743 · GitHub	CONFIRM	github.com	Issu
1370955 – (CVE-2016-6129) CVE-2016-6129 libtomcrypt: possible OP-TEE Bleichenbacher attack	CONFIRM	bugzilla.redhat.com	Issu
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

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