CVE-2018-12437

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-12437
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-15 02:29:00 UTC
Updated	2021-06-29 14:27:00 UTC
Description	LibTomCrypt through 1.18.1 allows a memory-cache side-channel attack on ECDSA signatures, aka the Return Of the Hidd

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Dropbear: Multiple vulnerabilities (GLSA 202007-53) — Gentoo security	GENTOO	security.gentoo.org	Third Party Adviso
www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-numbe...	MISC	www.nccgroup.trust	Exploit, Technical
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.report and Source URL Uptime Status status.cve.report