CVE-2017-1000413

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-1000413
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-02 17:29:00 UTC
Updated	2018-01-17 16:14:00 UTC
Description	Linaro's open source TEE solution called OP-TEE, version 2.4.0 (and older) is vulnerable a timing attack in the Montgomery

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linaro	Op-tee	All	All	All	All

References

Reference	Source	Link	Tags
Security Advisories. - OP-TEE	CONFIRM	www.op-tee.org	Vendor Advisory
optee_os/CHANGELOG.md at 2.5.0 · OP-TEE/optee_os · GitHub	CONFIRM	github.com	Third Party Advisory
Rsa for 2.5.0 by jbech-linaro · Pull Request #1610 · OP-TEE/optee_os · GitHub	CONFIRM	github.com	Third Party Advisory
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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