



CVE-2017-5681

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

Summary

CVE	CVE-2017-5681
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-07 18:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The RSA-CRT implementation in the Intel QuickAssist Technology (QAT) Engine for OpenSSL versions prior to 0.5.19 may

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intel	Quickassist Technology Engine	0.5.18	All	All	All
Application	Intel	Quickassist Technology Engine	0.5.18	All	All	All

References

Reference	Source	Link	Tags
Intel® Product Security Center	CONFIRM	security-center.intel.com	Patch, Vendor 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.

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