



CVE-2017-6952

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

Summary

CVE	CVE-2017-6952
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-16 21:59:00 UTC
Updated	2017-04-05 01:59:00 UTC
Description	Integer overflow in the cs_winkernel_malloc function in winkernel_mm.c in Capstone 3.0.4 and earlier allows attackers to ca

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Capstone-engine	Capstone	All	All	All	All

References

Reference	Source	Link
provide a validity check to prevent against Integer overflow conditio... · aquynh/capstone@6fe86ee · GitHub	CONFIRM	github.com
Capstone 'winkernel_mm.c' Integer Overflow Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
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, 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