



CVE-2022-39829

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

Summary

CVE	CVE-2022-39829
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-05 04:15:00 UTC
Updated	2022-09-08 03:44:00 UTC
Description	There is a NULL pointer dereference in aes256_encrypt in Samsung mTower through 0.3.0 due to a missing check on the r

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samsung	Mtower	All	All	All	All

References

Reference	Source	Link
/docs/manmaster/man3/EVP_CIPHER_CTX_new.html	MISC	www.openssl.org
Security: NULL Pointer Dereference in the function aes256_encrypt() · Issue #75 · Samsung/mTower · GitHub	MISC	github.com
mTower/ecdsa_keygen.c at 18f4b592a8a973ce5972f4e2658ea0f6e3686284 · Samsung/mTower · GitHub	MISC	github.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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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