

New issue

[Jump to bottom](#)

Security: NULL Pointer Dereference in the function aes256_encrypt() #75

 Closed

UVScan opened this issue on Sep 1 · 1 comment · Fixed by [#78](#)

Assignees



UVScan commented on Sep 1

Affected components

affected source code file: tools/ecdsa_keygen.c

Attack vector(s)

Lacking a check for the return value of EVP_CIPHER_CTX_new.
EVP_CIPHER_CTX_new() returns a pointer to a newly created EVP_CIPHER_CTX for success and NULL for failure.

Suggested description of the vulnerability for use in the CVE

Null pointer dereference vulnerability in aes256_encrypt() function in Samsung Electronics mTower v0.3.0 (and earlier) due to a missing check on the return value of EVP_CIPHER_CTX_new.

Discoverer(s)/Credits

UVScan


Reference(s)

https://www.openssl.org/docs/manmaster/man3/EVP_CIPHER_CTX_new.html

[mTower/tools/ecdsa_keygen.c](#)

Line 135 in 18f4b59

```
135     enc_ctx = EVP_CIPHER_CTX_new();
```

  **tdrozdovsky** self-assigned this on Sep 4

tdrozdovsky commented on Sep 4

Contributor


The issue will be reviewed and fixed as soon as possible.

  **tdrozdovsky** mentioned this issue on Sep 5


Fixed: lacking a check for the return value and NULL Pointer Dereference #78

 Merged

 9 tasks

 **tdrozdovsky** closed this as completed in [#78](#) on Sep 5

Assignees

 **tdrozdovsky**

Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fixed: lacking a check for the return value and NULL Pointer Dereference**
Samsung/mTower

2 participants

