

New issue

[Jump to bottom](#)

Security: Lacking a check for the return value of EC_KEY_set_public_key_affine_coordinates() #77

 Closed

UVScan opened this issue on Sep 1 · 1 comment

Assignees



UVScan commented on Sep 1

Affected components

affected source code file: tools/fwinfogen.c

Attack vector(s)

Lacking a check for the return value of EC_KEY_set_public_key_affine_coordinates.
EC_KEY_set_public_key_affine_coordinates() returns 1 on success or 0 on error.

Suggested description of the vulnerability for use in the CVE

DoS vulnerability in sign_pFwInfo() function in Samsung Electronics mTower v0.3.0 (and earlier) due to a missing check on the return value of EC_KEY_set_public_key_affine_coordinates.

Discoverer(s)/Credits

UVScan

Reference(s)

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

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

Line 194 in 18f4b59

194 `EC_KEY_set_public_key_affine_coordinates(eckey, x, y);`

tdrozdovsky commented on Sep 4

Contributor

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

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

  **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 on Sep 5

Assignees

 **tdrozdovsky**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

