

New issue

[Jump to bottom](#)

Security: Lacking a check for the return value of EC_KEY_set_private_key() #76

 Closed

UVScan opened this issue on Sep 1 · 1 comment

Assignees



UVScan commented on Sep 1

Affected components

affected source code file: tools/fwinfo.c

Attack vector(s)

Lacking a check for the return value of EC_KEY_set_private_key.

EC_KEY_set_private_key() returns 1 on success or 0 on error except when the priv_key argument is NULL, in that case it returns 0, for legacy compatibility, and should not be treated as an 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_private_key.

Discoverer(s)/Credits

UVScan


Reference(s)

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

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

Line 193 in 18f4b59

193 `EC_KEY_set_private_key(eckey, d);`

  **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 on Sep 5

Assignees

 **tdrozdovsky**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

