New issue

Jump to bottom

Security: Memory Allocation with Excessive Size Value in the function TEE_Malloc #74

Closed **c01dkit** opened this issue on Aug 1 · 1 comment

c01dkit commented on Aug 1 • edited

Affected components:

affected source code file: /tee/lib/libutee/tee_api.c, affected functions: TEE_Malloc

Attack vector(s)

To exploit the vulnerability, invoke the function TEE_Malloc and pass a large number to the parameter "len".

Suggested description of the vulnerability for use in the CVE

Memory Allocation with Excessive Size Value vulnerablity in TEE_Malloc function in Samsung Electronics mTower v0.3.0 (and earlier) allows a trusted application to trigger a Denial of Service (DoS) via invoking the function TEE_Malloc with an excessive number of the parameter "len".

Discoverer(s)/Credits

SyzTrust

Reference(s)

https://github.com/Samsung/mTower

mTower/tee/lib/libutee/tee_api.c
Line 314 in 18f4b59

```
314     void *TEE_Malloc(uint32_t len, uint32_t hint)
```

Additional information

The TEE_Malloc does not check the size of chunk to malloc. Executing the statement "tee_user_mem_alloc" with an excessive size value on a real IoT hardware (such as Numaker-PFM-M2351) will crash the trusted execution environment kernel and cause a Denial of Service (DoS).

Contact

c01dkit@outlook.com

tdrozdovsky commented on Aug 6 Contributor

Thanks for the analysis. I will check your issues. If you have ideas for fix, please create PRs

tdrozdovsky mentioned this issue on Oct 25

Fixed CVE-2022-38155, CVE-2022-40762 #86

Merged

9 tasks

tdrozdovsky closed this as completed 8 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants