__strlen_aarch64_mte frequently triggered problem with MTE

+1 Hotlists (1) Mark as Duplicate

Comments (2) Dependencies Duplicates (0) Blocking (0) Resources (5)

Infeasible Bug P2 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION we...@vivo.com created issue #1 Aug 25, 2023 04:44PM

Existing URLs containing the issue:
https://android.googlesource.com/platform/bionic/+/refs/heads/main/libc/arch-arm64/dynamic_function_dispatch.cpp

Description of issue (what needs changing):
From our practical experiences, so many Android Applications could trigger the MTE syncerrors and bring collapses only if we open the MTE, since the Android standard libc would use the MTE version strlen by default. The JNI interfaces which are used to pass strings bewteen native and JVM with `env->GetStringUTFChars` or `env->ReleaseStringUTFChars` could aggravate that.

```
#00 pc 00000000000937cc /apex/com.android.runtime/lib64/bionic/libc.so
(__strlen_aarch64_mte+12)
```

The developers' coding style or the compiler optimizations could make the string objects free ahead and of course, it is theoretically UAF (use after free). Something like the case below, in which the string object would be free because of some Return Value Optimization techniques of C++.

```
vector.push_back(toCppString(**).c_str())
```

I could understand the implementation consideration for this MTE version strlen. It is needed by completeness of theory and the MTE team may request the coverage of all dereerences from heap opeartions.

But I still have no idea whether it is necessary to bring MTE to the strlen? I think the stirng object is greatly management inherently and there is no need to operate memory explicitly. Although there are definetely certain UAF or other possible memory safety problems like OOB of string object caused by strlen, the real world impact maybe limited, especially with the Scudo's memory safety mitigations. Of course, this is just a sensory intuition and a concrete and rational analysis is essential.

So, is it possible to take some remedial actions or just disable the MTE strlen for better and more practical usage of MTE Android please?

Reporter	we...@vivo.com
Type	Bug
Priority	P2
Severity	S2
Status	Won't fix (Infeasible)
Access	Default access View
Assignee	nc...@google.com
Verifier	--
Collaborators	
CC	nc...@google.com sa...@google.com we...@vivo.com
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

✓ Links (5) Hide all

Links (5)

" https://android.googlesource.com/platform/bionic/+/refs/heads/main/libc/arch-arm64/dynami… "	we...@ #1
"…s component captures issues related to documentation ONLY on source.android.com , the website of the Android Open Source Proj… "	nc...@ #2
"https://source.android.com/setup/contribute/report-bugs"	nc...@ #2
"https://support.google.com/android/table/7393834 "	nc...@ #2
"For questions on github usage, refer to https://support.github.com/request/account?tags=dotcom-footer%2Chubberfy_account"	nc...@ #2

COMMENTS All comments Oldest first

nc...@google.com <nc...@google.com> #2 Sep 1, 2023 06:56AM

Status: Won't Fix (Infeasible)

This component captures issues related to documentation ONLY on source.android.com, the website of the Android Open Source Project.

For issues with the Android operating system, file a bug with the associated component found at:
https://source.android.com/setup/contribute/report-bugs

For user issues, find the right place to get help at the Android help center at
https://support.google.com/android/table/7393834

For questions on github usage, refer to https://support.github.com/request/account?tags=dotcom-footer%2Chubberfy_account