Proposal for C2x
WG14 n2464

Title:	Zero-size Reallocations are Undefined Behavior
Author, affiliation:	Robert C. Seacord, NCC Group
Date:	2019-09-10
Proposal category:	Defect
Target audience:	C programmers using the realloc functions

Abstract: Zero-size Reallocations are Undefined Behavior

Prior art: C

Zero-size Reallocations are Undefined Behavior

Reply-to: Robert C. Seacord (rcseacord@gmail.com)
Document No: n2464
Reference Document: N2433
Date: 2019-10-25

Summary of Changes

n2464

- Change 7.22.3.5 p3 to indicate that a call to `realloc` where size is zero is undefined behavior

Introduction and Rationale

DR400 was submitted as a result of the divergence of implementations of the realloc function as follows:

	Returns	**ptr**	**errno**
AIX			
`realloc(NULL,0)`	Always **NULL**		unchanged
`realloc(ptr,0)`	Always **NULL**	freed	unchanged
zOS			
`realloc(NULL,0)`	Always **NULL**		`ENOMEM`
`realloc(ptr,0)`	Always **NULL**	freed	`ENOMEM`
BSD			
`realloc(NULL,0)`	only gives **NULL** on alloc failure		`ENOMEM`
`realloc(ptr,0)`	only gives **NULL** on alloc failure	unchanged	`ENOMEM`
MSVC			

`realloc(NULL,0)`	only gives **NULL** on alloc failure		unchanged
`realloc(ptr,0)`	always returns **NULL**	freed	unchanged
glibc			
`realloc(NULL,0)`	only gives **NULL** on alloc failure		`ENOMEM`
`realloc(ptr,0)`	always returns **NULL**	freed	unchanged

This issue was resolved by loosening the requirements in the standard to allow for the existing range of implementations and included in C17.

N2438 Clarification Request requested further clarification of 7.22.3.5p4 the Returns section of the realloc function specification with a proposal to

Change 7.22.3.5 p3

The realloc function returns a pointer to the new object (which may have the same value as a pointer to the old object), or a null pointer if the new object has not been allocated.

to

The realloc function returns a pointer to the new object (which may have the same value as a pointer to the old object), or a null pointer to indicate a failure and that the new object has not been allocated.

Discussion at the Ithaca meeting and on the mailing list suggested that a call to `realloc` with a size of 0 be classified as undefined behavior.

POSIX currently states

Upon successful completion, `realloc()` shall return a pointer to the (possibly moved) allocated space. If size is 0, either:

- A null pointer shall be returned and, if `ptr` is not a null pointer, errno shall be set to an implementation-defined value.
- A pointer to the allocated space shall be returned, and the memory object pointed to by `ptr` shall be freed. The application shall ensure that the pointer is not used to access an object.

If there is not enough available memory, `realloc()` shall return a null pointer and set `errno` to [ENOMEM]. If `realloc()` returns a null pointer and errno has been set to [ENOMEM], the memory referenced by `ptr` shall not be changed.

Classifying a call to `realloc` with a size of 0 as undefined behavior would allow POSIX to define the otherwise undefined behavior however they please.

Proposed Wording

The wording proposed is a diff from the committee draft of ISO/IEC 9899-2017. Green text is new text, while ~~red~~ text is deleted text.

Change 7.22.3.5 p3 as follows:

If `ptr` is a null pointer, the `realloc` function behaves like the `malloc` function for the specified size. Otherwise, if `ptr` does not match a pointer earlier returned by a memory management function, or if the space has been deallocated by a call to the `free` or `realloc` function, or if `size` is zero, the behavior is undefined. If ~~size is nonzero and~~ memory for the new object is not allocated, the old object is not deallocated and its value is unchanged. ~~If size is zero and memory for the new object is not allocated, it is implementation-defined whether the old object is deallocated. If the old object is not deallocated, its value shall be unchanged.~~

Acknowledgements

I would like to recognize the following people for their help with this work: David Keaton and Aaron Ballman.

References

N2438 Realloc with size 0 ambiguity. http://www.open-std.org/jtc1/sc22/wg14/www/docs/n2438.htm