Proposal for C23
WG14 N 2800

Title:	calloc overflow handling
Author, affiliation:	Robert C. Seacord, NCC Group
Date:	2021-8-30
Proposal category:	Defect
Target audience:	Implementers
Abstract:	Explicitly define behavior on overflow in calloc
Prior art:	C

calloc overflow handling

Reply-to: Robert C. Seacord (rcseacord@gmail.com)
Document No: **N 2800**
Reference Document: N2699 (http://www.open-std.org/jtc1/sc22/wg14/www/docs/n2699.htm)
Date: 2021-8-30

Change Log

2021-8-30:

- Initial version

Introduction and Rationale

The current wording in the working draft (N2596 7.22.3.2.2) describes `calloc` as follows: "The `calloc` function allocates space for an array of `nmemb` objects, each of whose size is `size`. The space is initialized to all bits zero." In particular, regardless of whether or not the C expression `nmemb * size` overflows, `calloc` is not permitted to return a non-null pointer to fewer bytes than the mathematical product of `nmemb` and `size` (i.e., assuming infinitely ranged integers). According to Subclause 7.22.3.2 p2 "The `calloc` function allocates space for an array of `nmemb` objects, each of whose size is `size`" and according to Subclause 7.22.3 p1 "If the space cannot be allocated, a null pointer is returned." Implementations where overflow returned non-null values are non-conforming in the current draft standard.

RUS-CERT [RUS-CERT 2002, Weimer 2002] documented the defect in `calloc` implementations and similar routines:

> *Integer overflow can occur during the computation of the memory region size by calloc and similar functions. As a result, the function returns a buffer which is too small, possibly resulting in a subsequent buffer overflow.*

While most implementations were repaired, the standard was not updated to clarify the existing requirement.

The problem subsequently reoccurred [MSRC 2021]. The same vulnerability exists in standard memory allocation functions spanning widely used real-time operating systems (RTOS), embedded software development kits (SDKs), and C standard library (libc) implementations. These findings have been shared with vendors through responsible disclosure led by the Microsoft Security Response Center (MSRC) and the Department of Homeland Security (DHS), enabling these vendors to investigate and patch the vulnerabilities.

For a full list of affected products and CVEs, please visit the DHS website: ICSA-21-119-04 Multiple RTOS (https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04).

The purpose of this proposal is to clarify the existing behavior of `calloc` in the event that `nmemb * size` overflows, to help prevent future implementation defects resulting in security vulnerabilities.

Proposed Wording

The wording proposed is a diff from WG14 N2596. Green text is new text, while ~~red text~~ is deleted text.

First Wording

Change Subclause 7.22.3.2, “The **calloc** function” paragraph 3 to say

The **calloc** function returns either ~~a null pointer or~~ a pointer to the allocated space or a null pointer if the space cannot be allocated or nmemb * size overflows.

Second Wording

The **calloc** function returns either ~~a null pointer or~~ a pointer to the allocated space or a null pointer if the space cannot be allocated or the result of nmemb * size is not representable as a value of type size_t.

4.0 Acknowledgements

I would like to recognize the following people for their help with this work: David Goldblatt, Mark Santaniello, Florian Weimer, Erik Steringer, and Aaron Ballman.

5.0 References

[RUS-CERT 2002] RUS-CERT Advisory. Flaw in calloc and similar routines 2002-08:02. URL: https://web.archive.org/web/20081225201357/http://cert.uni-stuttgart.de/advisories/calloc.php

[Weimer 2002] Florian Weimer. RUS-CERT Advisory 2002-08:02: Flaw in calloc and similar routines. Mon, 05 Aug 2002. URL: https://www.opennet.ru/base/cert/1028651886_905.txt.html

[MSRC 2021] MSRC Team. “BadAlloc” – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks. April 29, 2021. URL: https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/