Hive Pro

THREAT ADVISORY

Multiple IoT devices affected by BadAlloc Vulnerabilities

TA202109

Threat Level Red

Publish Date – May 2, 2021

More than 25 vulnerabilities have been found in multiple IoT and OT devices which have been collectively named as BadAlloc Vulnerabilities. These Vulnerabilities reside in the standard memory allocation functions that are used in RTOS(real-time operating systems), SDKs(Software development kits) and C standard library implementations. These vulnerabilities could be easily exploited by attackers by executing malicious code and trigger DoS conditions. However, none of these vulnerabilities have been exploited as of now.

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2021-30636	Media Tek LinkIt SDK versions prior to 4.6.1	cpe:2.3:a:MediaTek-Labs:linkit_sdk:*:*:*:*:*:*:*:*	An integer overflow vulnerability in memory allocation pvPortCalloc(calloc) and pvPortRealloc(realloc), which can lead to memory corruption on the target device.	CWE-190
CVE-2021-27431	Arm CMSIS RTOS2 versions prior to 2.1.3	cpe:2.3:o:arm:cmsis-rtos2:2.1.*:*:*:*:*:*:*:* cpe:2.3:o:arm:cmsis-rtos2:2.0.0:*:*:*:*:*:*:* cpe:2.3:o:arm:cmsis-rtos2:0.02:*:*:*:*:*:*:*	An integer wrap-around vulnerbaility in osRtxMemoryAlloc (local malloc equivalent) function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or injected code execution.	
CVE-2021-27433	Arm mbed-uallaoc, Version 1.3.0	cpe:2.3:a:arm:mbed-uallaoc:1.3.0:*:*:*:*:*:*:*	An integer wrap-around vulnerability in function mbed_krbs, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-27435	Arm mbed OS, Version 6.3.0	cpe:2.3:o:arm:mbed_os:6.3.0:*:*:*:*:*:*:*	An integer wrap-around vulnerability in malloc_wrapper function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-27427	RIOT OS Versions 2020.01.1	cpe:2.3:a:riot_project:riot:2020.01:-:*:*:*:*:*:*	An integer wrap-around vulnerability in its implementation of calloc function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-22684	Samsung Tizen RT RTOS version 3.0.GBB		An integer wrap-around vulnerability in function s_calloc and mm_zalloc. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash.	
CVE-2021-27439	TencentOS-tiny Version 3.1.0		An integer wrap-around vulnerability in function 'tos_mmheap_alloc incorrect calculation of effective memory allocation size. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-27425	Cesanta Software Mongoose-OS v2.17.0	cpe:2.3:o:cesanta:mongoose_os:2.17.0:*:*:*:*:*:*:*	An integer wrap-around vulnerability in function mm_malloc. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2021-26461	Apache Nuttx OS Version 9.1.0	cpe:2.3:o:apache_foundation:nuttx_os:9.1.0:*:*:*:*:*:*:*	An integer wrap-around vulnerability in functions malloc, realloc and memalign. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	CWE-190
CVE-2020-35198	Windriver VxWorks, prior to 7.0	cpe:2.3:o:windriver:vxworks:5:*:*:*:*:*:*:* cpe:2.3:o:windriver:vxworks:6:*:*:*:*:*:*:*	A vulnerability found in the following functions; calloc(memLib), mmap/mmap64 (mmanLib), cacheDmaMalloc(cacheLib) and cacheArchDmaMalloc(cacheArchLib). This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2020-28895				
CVE-2021-31571	Amazon FreeRTOS Version 10.4.1	cpe:2.3:o:amazon_web_services:freertos:10.4.1:*:*:*:*:*:*:*	An integer wrap-around vulnerability in multiple memory management API functions (MemMang, Queue, StreamBuffer). This unverified memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-31572				
CVE-2021-27417	eCosCentric eCosPro RTOS Versions 2.0.1 through 4.5.3	cpe:2.3:o:ecoscentric:ecospro_rtos:*:*:*:*:*:*:*:*	An integer wrap-around vulnerability in function calloc (an implementation of malloc). The unverified memory assignment can lead to arbitrary memory allocation, resulting in a heap-based buffer overflow.	
CVE-2021-3420	Redhat newlib versions prior to 4.0.0	cpe:2.3:a:newlib_project:newlib:*:*:*:*:*:*:*:*	An integer wrap-around vulnerability in malloc and nano-malloc family routines (memalign, valloc, pvalloc, nano_memalign, nano_valloc, nano_pvalloc) due to insufficient checking in memory alignment logic. This insufficient checking can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	CWE-190, CWE-120
CVE-2021-27411	Micrium OS Versions 5.10.1 and prior	cpe:2.3:o:silicon_labs:micrium_os:*:*:*:*:*:*:*:*	An integer wrap-around vulnerability in functions Mem_DynPoolCreate, Mem_DynPoolCreateHW and Mem_PoolCreate. This unverified memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as very small blocks of memory being allocated instead of very large ones.	CWE-190
CVE-2021-26706	Micrium uCOS-II and uCOS-III Versions 1.39.0 and prior	cpe:2.3:o:silicon_labs:micrium_ucos-ii:1.39.0:*:*:*:*:*:*:* cpe:2.3:o:silicon_labs:micrium_ucos-iii:1.39.0:*:*:*:*:*:*:*	An integer wrap-around vulnerability in functions Mem_DynPoolCreate, Mem_DynPoolCreateHW and Mem_PoolCreate. This unverified memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as very small blocks of memory being allocated instead of very large ones.	
CVE-2021-27421	NXP MCUXpresso SDK versions prior to 2.8.2	cpe:2.3:a:nxp:mcuxpresso_sdk:*:*:*:*:*:*:*:*	An integer overflow vulnerability in SDK_Malloc function, which could allow to access memory locations outside the bounds of a specified array, leading to unexpected behavior such segmentation fault when assigning a particular block of memory from the heap via malloc.	
CVE-2021-22680	NXP MQX Versions 5.1 and prior		An integer overflow vulnerability in mem_alloc, _lwmem_alloc and _partition functions. This unverified memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-27419	Uclibc-NG, versions prior to 1.0.36		An integer wrap-around vulnerability in functions malloc-simple. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	
CVE-2021-27429	Texas Instrument TI-RTOS		An integer overflow vulnerability in 'HeapTrack_alloc' and result in code execution.	
CVE-2021-22636	Texas Instrument TI-RTOS		An integer overflow vulnerability in 'malloc' and result in code execution.	

Hive Pro

THREAT ADVISORY

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2021-27504	Texas Instrument devices running FREERTOS		An integer overflow vulnerability in 'malloc' for FreeRTOS, resulting in code execution.	CWE-190
CVE-2021-27502	Texas Instrument TI-RTOS		An integer overflow vulnerability in 'HeapMem_allocUnprotected' and result in code execution.	
Unassigned CVE	Google Cloud IoT Device SDK Version 1.0.2		A heap overflow due to integer overflow vulnerability in its implementation of calloc, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or code execution.	

Patch Links

https://github.com/FreeRTOS/FreeRTOS-Kernel/pull/224
https://github.com/apache/incubator-nuttx
https://github.com/ARMmbed/mbed-os/pull/14408
https://github.com/cesanta/mongoose-os
https://bugzilla.ecoscentric.com/show_bug.cgi?id=1002437
https://github.com/GoogleCloudPlatform/iot-device-sdk-embedded-c/pull/119/files
https://www.silabs.com/developers/micrium-os
https://mcuxpresso.nxp.com/en/welcome
https://sourceware.org/git/gitweb.cgi?p=newlib-cygwin.git
https://github.com/RIOT-OS/RIOT
https://github.com/Samsung/TizenRT
https://www.ti.com/technologies/security/report-product-security-vulnerabilities.html
https://www.ti.com/technologies/security/report-product-security-vulnerabilities.html
https://www.ti.com/technologies/security/report-product-security-vulnerabilities.html
https://downloads.uclibc-ng.org/releases/

References

https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04
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/
https://threatpost.com/microsoft-warns-25-critical-iot-industrial-devices/165752/