The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
04/30/2021

SUBJECT:
Multiple Vulnerabilities in Real-Time Operating Systems (RTOS) Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Real-Time Operating Systems (RTOS), the most severe of which could allow for remote code execution. RTOS is an operating system intended to serve real-time applications that process data as it comes in. Successful exploitation of the most severe of these vulnerabilities could result in remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Amazon FreeRTOS, Version 10.4.1
- Apache Nuttx OS, Version 9.1.0
- ARM CMSIS-RTOS2, versions prior to 2.1.3
- ARM Mbed OS, Version 6.3.0
- ARM mbed-uallaoc, Version 1.3.0
- Cesanta Software Mongoose OS, v2.17.0
- eCosCentric eCosPro RTOS, Versions 2.0.1 through 4.5.3
- Google Cloud IoT Device SDK, Version 1.0.2
- Linux Zephyr RTOS, versions prior to 2.4.0
- Media Tek LinkIt SDK, versions prior to 4.6.1
- Micrium OS, Versions 5.10.1 and prior
- Micrium uCOS II/uCOS III Versions 1.39.0 and prior
- NXP MCUXpresso SDK, versions prior to 2.8.2
- NXP MQX, Versions 5.1 and prior
- Redhat newlib, versions prior to 4.0.0
- RIOT OS, Version 2020.01.1
- Samsung Tizen RT RTOS, versions prior 3.0.GBB

- TencentOS-tiny, Version 3.1.0
- Texas Instruments CC32XX, versions prior to 4.40.00.07
- Texas Instruments SimpleLink MSP432E4XX
- Texas Instruments SimpleLink-CC13XX, versions prior to 4.40.00
- Texas Instruments SimpleLink-CC26XX, versions prior to 4.40.00
- Texas Instruments SimpleLink-CC32XX, versions prior to 4.10.03
- Uclibc-NG, versions prior to 1.0.36
- Windriver VxWorks, prior to 7.0

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Real-Time Operating Systems (RTOS), the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

Amazon FreeRTOS, Version 10.4.1
- Amazon FreeRTOS Version 10.4.1 is vulnerable to integer wrap-around 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-2021-31571 and CVE-2021-31572)

Apache Nuttx OS, Version 9.1.0
- Apache Nuttx OS Version 9.1.0 is vulnerable to integer wrap-around 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 (CVE-2021-26461)

ARM CMSIS-RTOS2, versions prior to 2.1.3
- Arm CMSIS RTOS2 versions prior to 2.1.3 are vulnerable to integer wrap-around inosRtxMemoryAlloc (local malloc equivalent) function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or injected code execution (CVE-2021-27431)

ARM mbed-uallaoc, Version 1.3.0
- Arm mbed-uallaoc memory library Version 1.3.0 is vulnerable to integer wrap-around 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-2021-27433)

Cesanta Software Mongoose OS, v2.17.0

- Cesanta Software Mongoose-OS v2.17.0 is vulnerable to integer wrap-around 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-2021-27425)

eCosCentric eCosPro RTOS, Versions 2.0.1 through 4.5.3

- eCosCentric eCosPro RTOS Versions 2.0.1 through 4.5.3 are vulnerable to integer wraparound 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-2021-27417)

Google Cloud IoT Device SDK, Version 1.0.2

- Google Cloud IoT Device SDK Version 1.0.2 is vulnerable to heap overflow due to integer overflow in its implementation of calloc, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or code execution

Media Tek LinkIt SDK, versions prior to 4.6.1

- Media Tek LinkIt SDK versions prior to 4.6.1 is vulnerable to integer overflow in memory allocation calls pvPortCalloc(calloc) and pvPortRealloc(realloc), which can lead to memory corruption on the target device (CVE-2021-30636)

Micrium OS, Versions 5.10.1 and prior

- Micrium OS Versions 5.10.1 and prior are vulnerable to integer wrap-around 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-2021-27411)

Micrium uCOS II/uCOS III Versions 1.39.0 and prior

- Micrium uCOS-II and uCOS-III Versions 1.39.0 and prior are vulnerable to integer wrap-around 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-2021-26706)

NXP MCUXpresso SDK, versions prior to 2.8.2

- NXP MCUXpresso SDK versions prior to 2.8.2 are vulnerable to integer overflow 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-2021-27421)

NXP MQX, Versions 5.1 and prior

- NXP MQX Versions 5.1 and prior are vulnerable to integer overflow 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-2021-22680)

Redhat newlib, versions prior to 4.0.0

- Redhat newlib versions prior to 4.0.0 are vulnerable to integer wrap-around 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 (CVE-2021-27411)

RIOT OS, Version 2020.01.1

- RIOT OS Versions 2020.01.1 is vulnerable to integer wrap-around 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-2021-27427)

Samsung Tizen RT RTOS, versions prior 3.0.GBB

- Samsung Tizen RT RTOS version 3.0.GBB is vulnerable to integer wrap-around in functions_calloc and mm_zalloc. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash (CVE-2021-22684)

TencentOS-tiny, Version 3.1.0

- TencentOS-tiny Version 3.1.0 is vulnerable to integer wrap-around 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-2021-27439)

Texas Instrument

- Texas Instrument TI-RTOS returns a valid pointer to a small buffer on extremely large values. This can trigger an integer overflow vulnerability in 'HeapTrack_alloc' and result in code execution (CVE-2021-27429)
- Texas Instrument TI-RTOS returns a valid pointer to a small buffer on extremely large values, which can trigger an integer overflow vulnerability in 'malloc' and result in code execution (CVE-2021-22636)
- Texas Instrument TI-RTOS, when configured to use HeapMem heap(default), malloc returns a valid pointer to a small buffer on extremely large values, which can trigger an integer overflow vulnerability in 'HeapMem_allocUnprotected' and result in code execution (CVE-2021-27502)
- Texas Instrument devices running FREERTOS, malloc returns a valid pointer to a small buffer on extremely large values, which can trigger an integer overflow vulnerability in 'malloc' for FreeRTOS, resulting in code execution (CVE-2021-27504)

Uclibc-NG, versions prior to 1.0.36

- uClibc-ng versions prior to 1.0.37 are vulnerable to integer wrap-around 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-2021-27419)

Windriver VxWorks, prior to 7.0

- Wind River VxWorks several versions prior to 7.0 firmware is vulnerable to weaknesses 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-2020-35198 and CVE-2020-28895)

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by the RTOS provider to vulnerable systems immediately after appropriate testing.
- Run all software as a nonprivileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept or execute files from untrusted and unknown sources.
- Remind users not to visit untrusted websites or follow links provided by untrusted or unknown sources.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
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/

CISA:
https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/microsoft-finds-critical-code-execution-bugs-in-iot-ot-devices/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31571
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31572
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26461
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27431
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27433
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27417
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27411
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22680
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27411

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27427
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22684
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27502
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27504
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27419
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35198
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28895