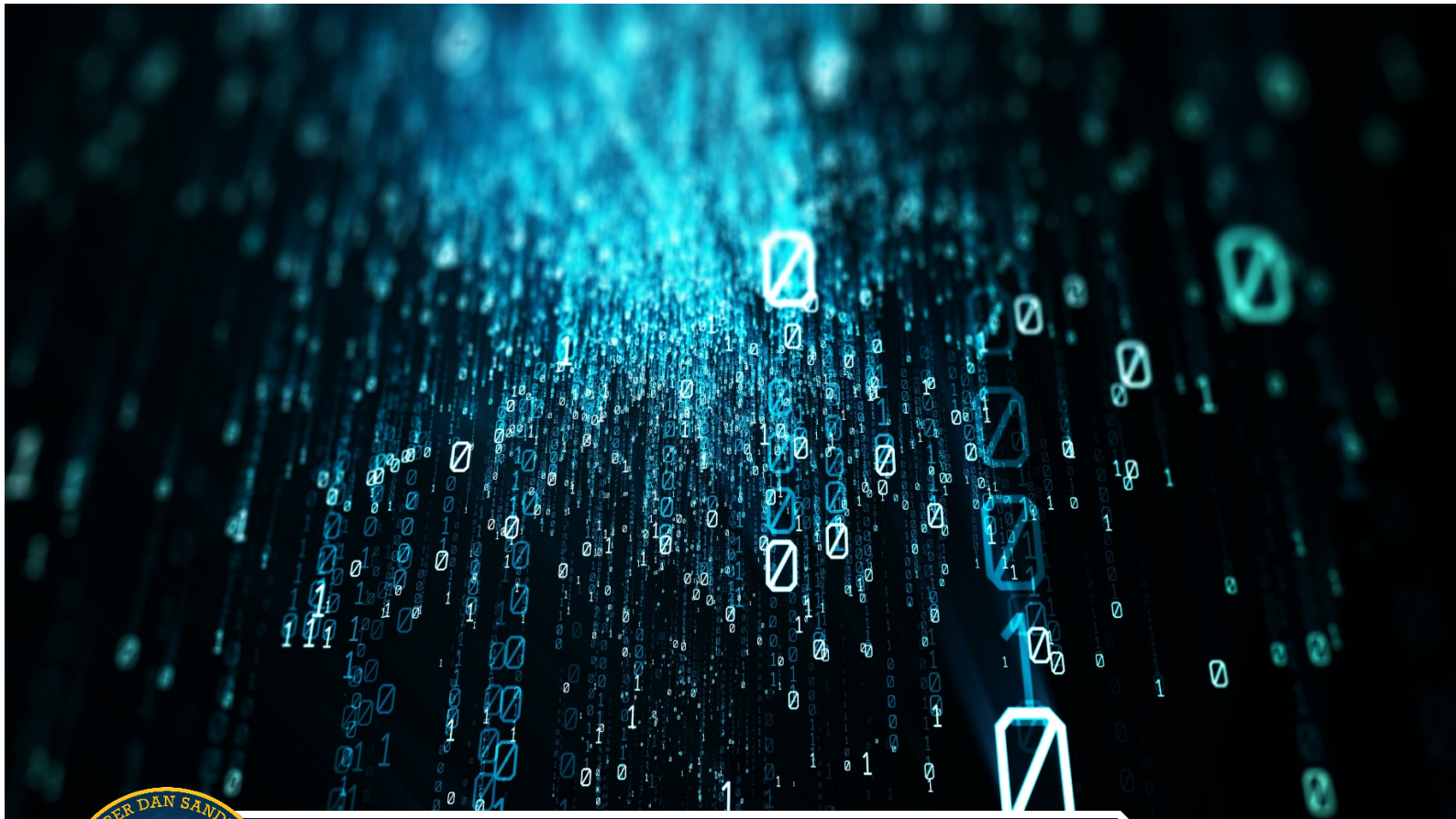

DIREKTORAT PROTEKSI INFRASTUKTUR INFORMASI KRITIKAL NASIONAL

DEPUTI BIDANG PROTEKSI

IMBAUAN KEAMANAN

'Bad Alloc' Multiple Vulnerabilities pada *Real-Time Operating System (RTOS):* Ancaman Terhadap Sistem IoT pada Lingkungan Industri

TLP:WHITE

PENDAHULUAN

Microsoft mempublikasikan beberapa kerentanan pada *Real-Time Operating System (RTOS),* kerentanan dengan tingkat *severity* tertinggi memungkinkan penyerang untuk melakukan eksekusi kode jarak jauh /*Remote Code Execution* (RCE). RTOS merupakan Sistem operasi yang umum digunakan pada *real time application* seperti *Internet of Things (IoT), Industrial Control System (ICS)* dan perangkat sejenis untuk memproses data. Kerentanan ini terjadi karena terdapat kesalahan proses validasi input pada implementasi *memory allocation* pada sistem/perangkat terdampak, dan di disebut juga sebagai "*BadAlloc*". Keberhasilan eksploitasi kerentanan akan memungkinkan penyerang untuk mendapatkan *privilege* sesuai dengan *privilege* korban yang sedang *logged-on* pada sistem atau perangkat. Kerentanan ini juga memungkinkan penyerang untuk *bypass security restriction,* serta membuat sistem atau perangkat *crash.* Penyerang dapat melakukan instalasi program, melihat, merubah atau menghapus data tergantung pada *permission* aplikasi tempat *exploit* berjalan.

RISIKO

Keberhasilan ekploitasi kerentanan oleh penyerang dapat mengakibatkan gangguan pada sistem atau produk terdampak seperti *crash* dan/ atau menungkinkan penyerang untuk melakukan *remote code injection / execution.*

RINCIAN TEKNIS KERENTANAN

Produk Terdampak

Berikut rincian produk yang terdampak kerentanan pada RTOS:

- Amazon FreeRTOS, Versi 10.4.1
- Apache Nuttx OS, Versi 9.1.0
- ARM CMSIS-RTOS2, versi sebelum 2.1.3
- ARM Mbed OS, Versi 6.3.0
- ARM mbed-uallaoc, Versi 1.3.0
- Cesanta Software Mongoose OS, v2.17.0

- eCosCentric eCosPro RTOS, Versi 2.0.1 hingga 4.5.3
- Google Cloud IoT Device SDK, Versi 1.0.2
- Linux Zephyr RTOS, versi sebelum 2.4.0
- Media Tek LinkIt SDK, versi sebelum 4.6.1
- Micrium OS, Versi 5.10.1 dan sebelumnya
- Micrium uCOS II / uCOS III Versi 1.39.0 dan sebelumnya
- NXP MCUXpresso SDK, versi sebelum 2.8.2
- NXP MQX, Versi 5.1 dan sebelumnya
- Redhat newlib, versi sebelum 4.0.0
- RIOT OS, Versi 2020.01.1
- Samsung Tizen RT RTOS, versi sebelumnya 3.0.GBB
- TencentOS-tiny, Versi 3.1.0
- Texas Instruments CC32XX, versi sebelum 4.40.00.07
- Texas Instruments SimpleLink MSP432E4XX
- Texas Instruments SimpleLink-CC13XX, versi sebelum 4.40.00
- Texas Instruments SimpleLink-CC26XX, versi sebelum 4.40.00
- Texas Instruments SimpleLink-CC32XX, versi sebelum 4.10.03
- Uclibc-NG, versi sebelum 1.0.36
- Windriver VxWorks, versi sebelum 7.0

Ringkasan Jenis Kerentanan

Integer Overflow or Wraparound CWE-190

1) **Media Tek LinkIt SDK versi sebelum 4.6.1** rentan terhadap *integer overflow* pada *memory allocation calls pvPortCalloc (calloc)* dan *pvPortRealloc (realloc)* yang dapat mengakibatkan *memory corruption*. Kerentanan ini memiliki kode **CVE-2021-30636 dan CVSSv3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L**.
2) **Arm CMSIS RTOS2 versi sebelum 2.1.3** memiliki kerentanan *integer wrap-around* pada fungsi *inosRtxMemoryAlloc (local malloc equivalent*), yang dapat menyebabkan *arbitrary memory allocation* sehingga mengakibatkan gangguan seperti *crash* atau dapat dilakukannya *injected code execution.* **Kerentanan ini**

memiliki kode CVE-2021-27431 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.

3) **Arm mbed-aulloac *memory library* versi 1.3.0** memiliki kerentanan *integer wrap-around* pada fungsi 'mbed_krbs', yang dapat menyebabkan *arbitrary memory allocation* sehingga mengakibatkan gangguan seperti *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-27433 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
4) **Produk Arm mbed versi 6.3.0** memiliki kerentanan *integer wrap-around* pada fungsi *'malloc_wrapper'*, yang mengakibatkan gangguan seperti *crash* atau dapat dilakukannya *remote code injection/execution* pada. **Kerentanan ini memiliki kode CVE-2021-27435 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
5) **RIOT OS versi 1.3.0** memiliki kerentanan *integer wrap-around* pada fungsi *calloc*, yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan seperti *crash* atau dapat dilakukannya *remote code injection/execution*. **Kerentanan ini memiliki kode CVE-2021-27427 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
6) **Samsung Tizen RT RTOS versi 3.0 GBB** memiliki kerentanan *integer wrap-around* pada fungsi *function_calloc*,dan *mm_zalloc* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* . **Kerentanan ini memiliki kode CVE-2021-22684 dan CVSS v3 *base score* 3.2 dengan *vector* CVSSv3: AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:L.**
7) **TencentOS-tiny versi 3.1.0** memiliki kerentanan *integer wrap-around* pada fungsi *tos_mmheap_alloc* karena terdapat kesalahan pada perhitungan ukuran alokasi memory efektif, yang dapat menyebabkan *arbitrary memory allocation.* sehingga dapat mengakibatkan gangguan seperti *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-27439 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**

8) **Cesanta Software Mongoose-OS v2.17.0** memiliki kerentanan *integer wrap-around* pada fungsi *mm_malloc* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-27425 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L**.
9) **Apache Nuttx OS Versi 9.1.0** memiliki kerentanan *integer wrap-around* pada fungsi *malloc, realloc* dan *memalign* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution*. **Kerentanan ini memiliki kode CVE-2021-26461 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L**.
10) **Firmware Wind River VxWorks sebelum Versi 9.1.0** memiliki kerentanan *integer wrap-around* pada fungsi *calloc(memLib), mmap/mmap64 (mmanLib), cacheDmaMalloc(cacheLib)* dan *cacheArchDmaMalloc(cacheArchLib)* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-35198 dan CVE-2020-28895 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
11) **Amazon FreeRTOS Versi 10.4.1** memiliki kerentanan *integer wrap-around* pada beberapa fungsi *memory management API* (*MemMang, Queue, StreamBuffer*) yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-31571 dan CVE-2021-31572 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
12) **eCosCentric eCosPro RTOS Versions 2.0.1 hingga 4.5.3** memiliki kerentanan *integer wrap-around* pada fungsi *calloc (*implementasi dari *malloc),* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan *heap-based buffer overflow*. **Kerentanan ini memiliki kode CVE-2021-3420 dan**

CVSS v3 *base score* 4.6 dengan *vector* CVSSv3: AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:H.

13) **Redhat newlib sebelum Versi 4.0.0** memiliki kerentanan *integer wrap-around* pada *family routines (memalign, valloc, pvalloc, nano_memalign, nano_valloc, nano_pvalloc),* dikarenakan kelemahan pada proses pemeriksaan *memory alignment logic.* kelemahan dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-3420 dan CVSS v3 *base score* 9.8 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.**
14) **Micrium OS versi 5.10.1 dan versi dibawahnya** memiliki kerentanan *integer wrap-around* pada fungsi Mem_DynPoolCreate, Mem_DynPoolCreateHW dan Mem_PoolCreate. Pengalokasian *memory* yang tidak terverifikasi dapat mengakibatkan *arbitrary memory allocation,* yang dapat menyebabkan gangguan pada pengalokasian *memory,* **kerentanan ini memiliki kode CVE-2021-27411 dan CVSS v3 *base score* 6.5 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L.**
15) **Micrium uCOS-II and uCOS-III versi 1.39.0 dan versi dibawahnya** memiliki kerentanan *integer wrap-around* pada fungsi Mem_DynPoolCreate, Mem_DynPoolCreateHW dan Mem_PoolCreate. Pengalokasian *memory* yang tidak terverifikasi dapat mengakibatkan *arbitrary memory allocation,* yang dapat menyebabkan gangguan pada pengalokasian *memory,* **kerentanan ini memiliki kode CVE-2021-26706 dan CVSS v3 *base score* 6.5 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L.**
16) **NXP MCUXpresso SDK versi dibawah 2.8.2** memiliki kerentanan *integer overflow* pada fungsi SDK_Malloc yang memungkinkan untuk mengakses lokasi memori diluar batas *array* yang ditentukan, hal tersebut dapat mengakibatkan gangguan seperti kesalahan segmentasi saat menetapkan blok memori tertentu dari *heap* melalui *malloc.* **Kerentanan ini memiliki kode CVE-2021-27421,CVSS v3 dan *base score* 6.5 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L.**

17) **NXP MQX Versions 5.1 dan versi dibawahnya** memiliki kerentanan *integer overflow* pada *mem_alloc, _lwmem_alloc* dan *_partition functions* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution.* **Kerentanan ini memiliki kode CVE-2021-26680, dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
18) **uClibc-ng dibawah versi 1.0.37** memiliki kerentanan *integer wrap-arround* pada fungsi *malloc-simple* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *remote code injection/execution*. **Kerentanan ini memiliki kode CVE-2021-27419 dan CVSS v3 *base score* 7.3 dengan *vector* CVSSv3: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.**
19) **Texas Instrument TI-RTOS** memiliki kerentanan *integer overflow* pada 'HeapTrack_alloc' sehingga dapat mengakibatkan dapat dilakukannya *code execution.* **Kerentanan ini memiliki kode CVE-2021-27429 dan CVSS v3 *base score* 7.4 dengan *vector* CVSSv3: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.**
20) **Texas Instrument TI-RTOS** memiliki kerentanan *integer overflow* pada fungsi '*malloc*' sehingga dapat mengakibatkan dapat dilakukannya *code execution*. **Kerentanan ini memiliki kode CVE-2021-22636, dan CVSS v3 *base score* 7.4 dengan *vector* CVSSv3: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.**
21) **Perangkat Texas Instrument yang menjalankan FREERTOS** memiliki kerentanan *integer overflow* pada fungsi '*malloc'* untuk FREERTOS yang dapat *code execution.* **Kerentanan ini memiliki kode CVE-2021-27504 dan CVSS v3 *base score* 7.4 dengan *vector* CVSSv3: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.**
22) **Texas Instrument, ketika dikonfigurasi menggunakan *HeapMem heap(default)***, *malloc* mengembalikan *valid pointer* ke sebuah ukuran *buffer* yang kecil dengan nilai yang sangat besar yang dapat mengakibatkan kerentanan *overflow vulnerability* pada *'HeapMem_allocUnprotected'* dan memungkinkan *code execution.* **Kerentanan ini memiliki *kode CVE-2021-27502 dan CVSS v3 base score 7.4 dengan vector CVSSv3: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.***

23) *Google Cloud IoT Device SDK Versi 1.0.2* rentan terhadap *heap overflow* karena terdapat *integer overflow* pada implementasi *calloc,* yang dapat menyebabkan *arbitrary memory allocation* sehingga dapat mengakibatkan gangguan *crash* atau dapat dilakukannya *code execution*. Google PSIRT akan menetapkan CVE dan skor CVSS akan dihitung saat CVE telah ditetapkan.

LANGKAH MITIGASI KERANTANAN

BSSN merekomendasikan pengguna perangkat IoT atau sistem kontrol yang memiliki kerentanan pada Imbauan keamanan ini agar melakukan langkah pelindungan untuk memperkecil peluang eksploitasi dari kerentanan ini. Berikut beberapa langkah yang dapat dilakukan:

1. Menerapkan pembaruan (*update*) yang telah disediakan oleh *vendor*, berikut beberapa informasi status pembaruan yang terkait perangkat IoT terdampak:
   - *Amazon FreeRTOS – Update available*
   - *Apache Nuttx OS Version 9.1.0 – Update available*
   - *ARM CMSIS-RTOS2 – Update in progress, expected in June*
   - *ARM Mbed OS – Update available*
   - *ARM mbed-uallaoc – no longer supported and no fix will be issued*
   - *Cesanta Software mongooses – Update available*
   - *eCosCentric eCosPro RTOS: Update to Versions 4.5.4 and newer – Update available*
   - *Google Cloud IoT Device SDK – Update available*
   - *Media Tek LinkIt SDK – MediaTek will provide the update to users. No fix for free version, as it is not intended for production use.*
   - *Micrium OS: Update to v5.10.2 or later – Update available*
   - *Micrium uCOS-II/uCOS-III: Update to v1.39.1 – Update not yet released*
   - *NXP MCUXpresso SDK – Update to 2.9.0 or later*
   - *NXP MQX – update to 5.1 or newer*
   - *Redhat newlib – Update available*
   - *RIOT OS – Update availableSamsung Tizen RT RTOS – Update available*
   - *TencentOS-tiny – Update available*

- *Texas Instruments CC32XX – Update to v4.40.00.07*
- *Texas Instruments SimpleLink CC13X0 – Update to v4.10.03*
- *Texas Instruments SimpleLink CC13X2-CC26X2 – Update to v4.40.00*
- *Texas Instruments SimpleLink CC2640R2 – Update to v4.40.00*
- *Texas Instruments SimpleLink MSP432E4 – Confirmed. Belum tersedia pembaruan*
- *uClibc-ng – Update available*
- Windriver VxWorks – dalam proses *update*

2. Minimalkan eksposur jaringan untuk semua perangkat dan/atau sistem kontrol yang terdampak, dan pastikan tidak dapat diakses dari jaringan Internet.
3. Melakukan identifikasi sistem kontrol dan perangkat jarak jauh terdampak kerentanan dengan posisi dibelakang *firewall* serta lakukan pemisahan jaringan dari segmen jaringan bisnis.
4. Jika akses terhadap perangkat sistem kontrol memerlukan akses jarak jauh, gunakan metode akses jarak jauh yang aman, seperti penggunaan *Vitual Private Network* (VPN), serta memastikan bahwa perangkat/perangkat VPN yang digunakan tidak memiliki kerentanan.

REFERENSI

[1] US-CERT CISA DHS, "ICS Advisory (ICSA-21-119-04)," CISA DHS, 04 Mei 2021. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04. [Accessed 05 Mei 2021].

[2] Canadian Center for Cyber Security, "[Control Systems] Multiple RTOS Security Vulnerabilities," 30 April 2021. [Online]. Available: https://cyber.gc.ca/en/alerts/control-systems-multiple-rtos-security-vulnerabilities. [Accessed 05 Mei 2021].

[3] E. Montalbano, "Microsoft Warns of 25 Critical Vulnerabilities in IoT, Industrial Devices," threatpost.com, 30 April 2021. [Online]. Available:

https://threatpost.com/microsoft-warns-25-critical-iot-industrial-devices/165752/. [Accessed 05 Mei 2021].

[4] Microsoft Security Response Center (MSRC) Team, ""BadAlloc" – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks," Microsoft, 29 April 2021. [Online]. Available: 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/. [Accessed 05 Mei 2021].