CVE-2021-21836

Explotación de Vulnerabilidades Software
Máster Universitario en Ingeniería Informática
Juan Asensio Ayesa

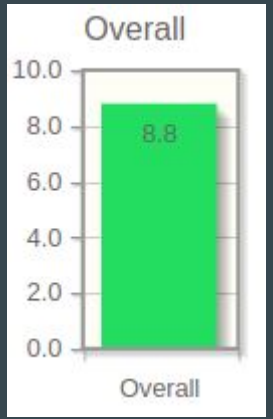
Contexto

- Librería Open Source tratamiento de datos multimedia
- Centrada en cumplir estándares
- Más de 20 años de desarrollo

1. https://github.com/gpac/gpac
2. https://gpac.wp.imt.fr/

Caracterización de la vulnerabilidad

- Función ctts_box_read()
  - Encargada de la decodificación de un archivo MP4
  - Se ejecuta con el código FOURCC ‘ctts’
- Afecta a la versión 1.0.1
- Se puede producir un Integer overflow en sistemas de 32 bits
  - El resultado de esa operación aritmética es usado para reservar memoria
- Overall 8.8, riesgo alto



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

1. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2021-21836&vector=AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H&version=3.1&source=NIST

1. https://talosintelligence.com/vulnerability_reports/TALOS-2021-1297

Descripción técnica I

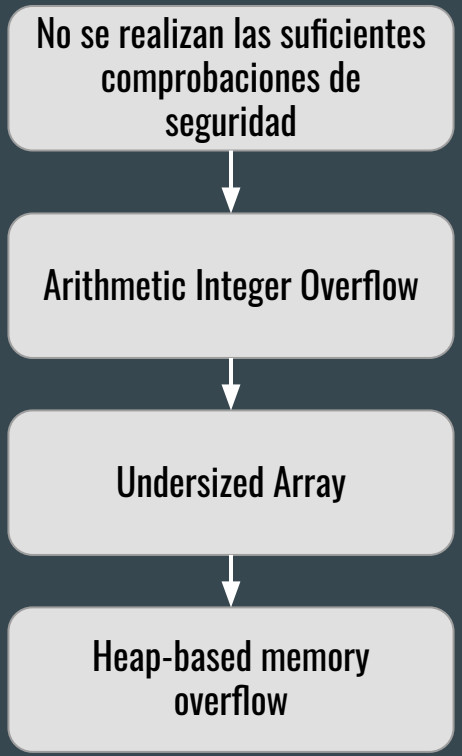
```
src/isomedia/box_code_base.c:386
GF_Err ctts_box_read(GF_Box *s, GF_BitStream *bs)
{
    u32 i;
    u32 sampleCount;
    GF_CompositionOffsetBox *ptr = (GF_CompositionOffsetBox *)s;

    ISOM_DECREASE_SIZE(ptr, 4);
    ptr->nb_entries = gf_bs_read_u32(bs);                                   // [20] read u32 from input

    if (ptr->nb_entries > ptr->size / 8) {                                  // [20] check entries againsti nput
        GF_LOG(GF_LOG_ERROR, GF_LOG_CONTAINER, ("[iso file] Invalid number of entries %d in ctts\n", ptr->nb_entries));
        return GF_ISOM_INVALID_FILE;
    }

    ptr->alloc_size = ptr->nb_entries;                                      // [21] assign number of entries to "alloc_size"
field
    ptr->entries = (GF_DttsEntry *)gf_malloc(sizeof(GF_DttsEntry)*ptr->alloc_size);     // [20] calculate size of allocation using
"alloc_size" field
    if (!ptr->entries) return GF_OUT_OF_MEM;
    sampleCount = 0;
    for (i=0; i<ptr->nb_entries; i++) {
        ISOM_DECREASE_SIZE(ptr, 8);
        ptr->entries[i].sampleCount = gf_bs_read_u32(bs);                   // [22] read entries from atom into undersized array
        if (ptr->version)
            ptr->entries[i].decodingOffset = gf_bs_read_int(bs, 32);
        else
            ptr->entries[i].decodingOffset = (s32) gf_bs_read_u32(bs);
...
    }
...
    return GF_OK;
}
```

Descripción técnica II



Mitigación

1. https://github.com/gpac/gpac/blob/master/src/isomedia/box_code_base.c

```
387  GF_Err ctts_box_read(GF_Box *s, GF_BitStream *bs)
388  {
389          u32 i;
390          u32 sampleCount;
391          GF_CompositionOffsetBox *ptr = (GF_CompositionOffsetBox *)s;
392
393          ISOM_DECREASE_SIZE(ptr, 4);
394          ptr->nb_entries = gf_bs_read_u32(bs);
395
396          if (ptr->nb_entries > ptr->size / 8 || (u64)ptr->nb_entries > (u64)SIZE_MAX/sizeof(GF_DttsEntry) ) {
397                  GF_LOG(GF_LOG_ERROR, GF_LOG_CONTAINER, ("[iso file] Invalid number of entries %d in ctts\n", ptr->nb_entries));
398                  return GF_ISOM_INVALID_FILE;
399          }
```

Intento de Exploit

- Crear Vídeo MP4 que provocase el crash del programa
  - Cocinado del propio vídeo mediante librerías de python
    - **La librería ffmpeg local fallaba con FOURCC ctts**
- Ajustado de un vídeo existente para utilizar el FOURCC correcto
  - Modificación del FOURCC mediante python
    - Mismo fallo que con el otro método
  - Utilización de programas ya existentes
    - **No permitían utilizar el código FOURCC necesario**
- Uso de código proporcionado por TALOS
  - Permite cambiar los metadatos del vídeo a generar
  - **Mismo fallo que en los casos anteriores**

¿Preguntas?