### Suricata - Bug #1843

**Mpm Ac: int overflow during init**

<table>
<thead>
<tr>
<th>07/12/2016 04:57 AM - i3 here</th>
</tr>
</thead>
</table>

| Status: | Closed |
| Priority: | Normal |
| Assignee: | Sascha Steinbiss |
| Category: |  |
| Target version: | 3.2.1 |
| Affected Versions: |  |

**Description**

SCRealloc failed: Cannot allocate memory, while trying to allocate 18446744071562067968 bytes

```c
static inline int SCACBSInitNewState(MpmCtx *mpm_ctx)
{
    void *ptmp;
    SCACBSCtx *ctx = (SCACBSCtx *)mpm_ctx->ctx;
    int ascii_code = 0;
    int size = 0;

    /* reallocate space in the goto table to include a new state */
    size = (ctx->state_count + 1) * ctx->single_state_size;
    ptmp = SCRealloc(ctx->goto_table, size);

    //size is a int
    but (ctx->state_count + 1) * ctx->single_state_size; is a unsigned int
    when the size > 2G
    size is overflow
```

**History**

**#1 - 07/12/2016 05:16 AM - Victor Julien**

- Description updated

**#2 - 07/12/2016 05:23 AM - Victor Julien**

What kind of rules do you use to get this issue?

**#3 - 07/12/2016 05:49 AM - i3 here**

Victor Julien wrote:

What kind of rules do you use to get this issue?

like this, the number of 36,000.

alert http any any -> any any (msg:"xxxxxxxxxxxxxxxxx"; content:"[6F 88 6E 0D 60 69 88 66 6C 83 60 66 62 49 6E 63 68 02 60 0A 64 66 88 84 48 66
69 68 68 84 02 0C 00 66 64 60 61 61 66 66 6C 31 04 4C 66 68 84 02 00 03 64 6F 80 02 00 06 68 69 64 68 68 02 29 06 48 66 69
68 64 02 29 06 68 64 61 62 4F 82 64 66 82 02 00 00 0C 64 49 64 64 43 60 43 6C 69 66 6E 84 11 41 86 84 4C 6F 68 69 6E 64 43 60 43
6C 69 66 6E 84 0D 4D 61 88 4C 69 6E]; classtype:trojan-activity; sid:60000021; rev:1;)

**#4 - 07/12/2016 09:11 AM - Peter Manev**

The err msg is the same as reported in - [https://redmine.openinfosecfoundation.org/issues/1827](https://redmine.openinfosecfoundation.org/issues/1827). Would it be related?

**#5 - 07/21/2016 03:09 PM - Andreas Herz**

- Assignee set to OISF Dev

---

09/04/2022 1/2
#6 - 02/09/2017 06:28 AM - Victor Julien
- Target version set to TBD
- Status changed from New to Closed
- Assignee changed from OISF Dev to Sascha Steinbiss
- Target version changed from TBD to 3.2.1

https://github.com/inliniac/suricata/pull/2548

#7 - 02/13/2017 10:15 AM - Victor Julien
- Subject changed from suricata int overflow to Mpm Ac: int overflow during init