New issue

Jump to bottom

NULL dereference on memory allocation error (src/ flb_avro) #3044

Closed raminfp opened this issue on Feb 9, 2021 · 3 comments

raminfp commented on Feb 9, 2021

Bug Report

Describe the bug

NULL dereference (value returned by flb_malloc is not checked) after memory allocation error (flb_malloc is wrapper on malloc returning NULL on unsuccessful allocation).
In most cases this issue will lead to crash via segmentation fault.

Vulnerable Code

```
flb_sds_t flb_msgpack_raw_to_avro_sds(const void *in_buf, size_t in_size, struct flb_avro_fields *ctx)
{
    msgpack_unpacked result;
    msgpack_object *root;

    size_t avro_buffer_size = in_size * 3;
    char *out_buff = flb_malloc(avro_buffer_size);

    .... SKIP.....

   flb_debug("before avro_writer_memory\n");
    awriter = avro_writer_memory(out_buff, avro_buffer_size);
    if (awriter == NULL) {
```

To Reproduce
Problem was identified by source code review.

Expected behavior

Memory allocation errors should be handled by checking value returned by flb_malloc().

Your Environment

- Version used:
  Current "master" branch

Additional context

See following recommendations for details:
https://wiki.sei.cmu.edu/confluence/display/c/ERR33-C.+Detect+and+handle+standard+library+errors

yongtang mentioned this issue on Feb 9, 2021

Add additional check returned from flb_malloc #3045

Merged

3 tasks

yongtang commented on Feb 9, 2021 Contributor

Thanks **@raminfp** , added a PR #3045 for the fix.

edsiper commented on Feb 9, 2021 Member

thanks, #3045 has been merged

edsiper closed this as completed on Feb 9, 2021

abergmann commented on Feb 11, 2021

CVE-2021-27186 was assigned to this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants