New issue

Jump to bottom

An unsafe operation is found in the S2J_STRUCT_GET_string_ELEMENT function #13

Closed marckwei opened this issue on Nov 18, 2020 · 5 comments

marckwei commented on Nov 18, 2020

struct2json

Vulnerability Analysis

An unsafe operation is found in the `S2J_STRUCT_GET_string_ELEMENTfunction` . The `strcpy` function is used to copy `JSON->value` to the `struct` , which may cause overflow when `JSON->value` is longer than structure defined array size.

POC

```
#include "s2j.h"
#include <stdint.h>
#include <stdio.h>

typedef struct {
  char name[8];
} Hometown;

static void *json_to_struct(cJSON* json_obj) {
  /* create Hometown structure object */
  s2j_create_struct_obj(struct_hometown, Hometown);

  /* deserialize data to Hometown structure object. */
  s2j_struct_get_basic_element(struct_hometown, json_obj,string, name);
  return struct_hometown;
}


int main(void) {
  cJSON * json=NULL;

  json=cJSON_CreateObject();

  cJSON_AddStringToObject(json, "name", "ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ");

  Hometown * test=json_to_struct(json);

  printf("that\'s fine!%zu",sizeof(test));


  return 0;
}
```

Run:

Suggestion

Use `strncpy` instead of `strcpy` to control the length of `JSON->value` :

```
#define S2J_STRUCT_GET_string_ELEMENT(to_struct, from_json, _element) \
  json_temp = cJSON_GetObjectItem(from_json, #_element); \
  if (json_temp) strncpy((to_struct)->_element, json_temp->valuestring,sizeof((to_struct)->_element));
```

After modification:

1

libradoge commented on Dec 28, 2020 Contributor

字符串的话，是否要修改成：sizeof是否要-1：

```
#define S2J_STRUCT_GET_string_ELEMENT(to_struct, from_json, _element) \
  json_temp = cJSON_GetObjectItem(from_json, #_element); \
  if (json_temp) strncpy((to_struct)->_element, json_temp->valuestring,sizeof((to_struct)->_element) -1 );
```

abergmann commented on Dec 28, 2020

CVE-2020-29203 was assigned to this issue.

armink commented on Dec 28, 2020 — Owner

Thanks for your feedback, can you submit a PR for it?

libradoge commented on Dec 28, 2020 — Contributor

> Thanks for your feedback, can you submit a PR for it?

It's my first time to submit a PR, so please check my work carefully...And thank you for giving me this chance!

armink mentioned this issue on Dec 28, 2020

Modify the length of strncpy #15

Merged

armink commented on Dec 28, 2020 — Owner

> Thanks for your feedback, can you submit a PR for it?
>
> It's my first time to submit a PR, so please check my work carefully...And thank you for giving me this chance!

Good job.

Thank you for your contribution, PR has been merged

armink closed this as completed on Dec 28, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants