[CVE-2020-26800] Stack based buffer overflow while parsing JSON file #5917

Open **Cr0wTom** opened this issue on Jan 10, 2021 · 2 comments

Cr0wTom commented on Jan 10, 2021 • edited

Short description

Stack based buffer overflow while parsing JSON file Leads to DoS

Attack scenario

An attacker can supply a specially crafted config.json file, consisting of 3764 left square brackets or more, which results in segmentation fault by the application. This immediately results in Denial of Service, and with more advanced exploitation it can have further implications, with higher severity security issues.

Components

Aleth 1.8.0

Reproduction

Create a .json file consisting of 3764 left square brackets ([) or more. Run it using the following command; `./aleth --config` followed by the .json file created earlier.

The stack overflow can be examined with gdb (`set args --config ./test.json`) or with valgrind (`valgrind ./aleth --config ./test3.json`).

I submitted this bug in the bug bounty program in Oct 05, 2020, but that kind of vulnerabilities are out of scope. As there was no intention to publish the vulnerability and issue a fix after 3 months I responsibly disclose the vulnerability with the intention to help the security team to fix the issue or mark the application as EOL if that's the case. As I didn't manage to properly compile the app with my fuzzers compiler I could use some insights on where the parser of the config file is.

In any case, I would be happy to help and assist with the issue.

Edit/Update: Github Issue creation for the issue has been approved.

Edit/Update 2: CVE has been issued. I will update once it is public.

Edit/Update 3: CVE has been published: https://nvd.nist.gov/vuln/detail/CVE-2020-26800

Cr0wTom changed the title ~~Stack based buffer overflow while parsing JSON file~~ **[CVE-2020-26800] Stack based buffer overflow while parsing JSON file** on Jan 11, 2021

OS-WS commented on Apr 21, 2021

Hi, was this issue ever addressed?

Cr0wTom commented on Apr 21, 2021 Author

> Hi, was this issue ever addressed?

Hello, as far as i understand the project is dead and I don't believe that a fix is planned.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants