Closed Issue created 2 years ago by Casper Sun

CVE-2020-12825: Stack overflow in cr_parser_parse_any_core in cr-parser.c

Too many recursion in function `cr_parser_parse_any_core` could cause stack overflow, if attacker provides many '('.

reproduce step:

1. compile libcroco with ASAN
2. run poc using command `./csslint-0.6 poc`

poc: poc

result:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==34840==ERROR: AddressSanitizer: stack-overflow on address 0x7fff6fd36fe8 (pc 0x0000004d9119 bp 0x000000000048 sp 0x7
fff6fd36fc0 T0)
    #0 0x4d9118 in __sanitizer::StackDepotPut(__sanitizer::StackTrace) /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/proje
cts/compiler-rt/lib/sanitizer_common/sanitizer_stackdepot.cc:97
    #1 0x4255ad in __asan::Allocator::Allocate(unsigned long, unsigned long, __sanitizer::BufferedStackTrace*, __asan:
:AllocType, bool) /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_allocator.cc:509
    #2 0x4265b6 in __asan::asan_malloc(unsigned long, __sanitizer::BufferedStackTrace*) /home/casper/fuzz/fuzzdeps/llv
m-9.0.0.src/projects/compiler-rt/lib/asan/asan_allocator.cc:875
    #3 0x4a8883 in malloc /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc
:146
    #4 0x539891 in cr_token_new /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-token.c:138:18
    #5 0x53f30b in cr_tknzr_get_next_token /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-tknzr.c:2007:17
    #6 0x50db42 in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1179:18
    #7 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #8 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #9 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #10 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #11 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #12 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #13 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #14 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #15 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #16 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #17 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    #18 0x50e43f in cr_parser_parse_any_core /home/casper/targets/gramma/libcroco/afl/BUILD/src/cr-parser.c:1240:34
    ...
```

Edited 2 years ago by Simon McVittie

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Related merge requests 2

○ parser: limit recursion in block and any productions

!5

libcroco: limit recursion in block and any productions (CVE-2020-12825)

GNOME/gnome-shell!1404 ✓

When these merge requests are accepted, this issue will be closed automatically.

Activity

Simon McVittie changed title from **Stack overflow in cr_parser_parse_any_core in cr-parser.c** to **CVE-2020-12825: Stack overflow in cr_parser_parse_any_core in cr-parser.c** 2 years ago

Simon McVittie @smcv · 2 years ago

According to downstream bug https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=960527 this is CVE-2020-12825.

Michael Catanzaro @mcatanzaro · 2 years ago

I fear this is likely the tip of the iceberg for libcroco. E.g. cr_parser_parse_block_core() is also obviously recursive with no apparent limit on how many times it can be called.

I'll add some naive counter, but keep in mind this library is dead and it's time for distros to drop it. I attempted to retire it from Fedora today but was thwarted by cinnamon, which still uses it.

Michael Catanzaro @mcatanzaro · 2 years ago

I looked up the CSS spec to try to visualize what productions can call each other: https://www.w3.org/TR/CSS2/syndata.html#tokenization.

```
stylesheet  : [ CDO | CDC | S | statement ]*;
statement   : ruleset | at-rule;
at-rule     : ATKEYWORD S* any* [ block | ';' S* ];
block       : '{' S* [ any | block | ATKEYWORD S* | ';' S* ]* '}' S*;
ruleset     : selector? '{' S* declaration? [ ';' S* declaration? ]* '}' S*;
selector    : any+;
declaration : property S* ':' S* value;
property    : IDENT;
value       : [ any | block | ATKEYWORD S* ]+;
any         : [ IDENT | NUMBER | PERCENTAGE | DIMENSION | STRING
              | DELIM | URI | HASH | UNICODE-RANGE | INCLUDES
              | DASHMATCH | ':' | FUNCTION S* [any|unused]* ')'
              | '(' S* [any|unused]* ')' | '[' S* [any|unused]* ']'
              ] S*;
unused      : block | ATKEYWORD S* | ';' S* | CDO S* | CDC S*;
```

I think only `block` and `any` are problematic. According to this grammar, both can also be called via `value`, and `block` can be called via `unused`. I don't see `unused` anywhere in cr-parser.c, though. And nothing can call `value` recursively. So I think we only need to limit calls to `block` and `any`, and the limit can begin at `value`.

CC @chpe in case you want to give a second opinion. I know you're not a libcroco maintainer anymore, but you're active in GNOME and I suspect the devs listed as the current maintainers don't have GitLab accounts.

Michael Catanzaro @mcatanzaro · 2 years ago

Oh @icq ! You've worked on libcroco too! Hi there. D:

Michael Catanzaro mentioned in commit 6eb257e5 2 years ago

Michael Catanzaro mentioned in merge request !5 2 years ago

Christian Persch @chpe · 2 years ago

I haven't looked at libcroco in a long time.

Given that this is not the even only security issue filed here, and there are likely many more lurking, I don't think it's a good use of anyone's time to keep alive a project that is only used anymore by a non-gnome desktop. You could ask cinnamon to take it over, or simply archive it.

Michael Catanzaro @mcatanzaro · 2 years ago

We managed to retire the Fedora package after all. Fedora's cinnamon will bundle libcroco, like upstream gnome-shell already does. It's also bundled (upstream) by gettext. These projects ought to migrate to something different.

Ignacio Casal Quinteiro @icq · 2 years ago

Yeah, this project is insecure and not maintained anymore. The reason I made some releases was that there were patches standing in bugzilla and it was needed at the time. Now that most of the projects are ported to something else I would say this project should just die. That said if there is a real reason to make a patch and a release then maybe we should do it. Dunno...

Michael Catanzaro @mcatanzaro · 2 years ago

Probably better to archive the project, to avoid misplaced expectations. If can ask sysadmins to do this if there are no objections. Distros can pick up any patches downstream anyway.

Simon McVittie @smcv · 2 years ago

> Fedora's cinnamon will bundle libcroco, like upstream gnome-shell already does. It's also bundled (upstream) by gettext. These projects ought to migrate to something different.

Those two projects are also the only ones in Debian testing/unstable still using libcroco, and I've opened Debian bugs recommending that they do the same as in Fedora for now.

Has anyone from (what remains of) libcroco upstream reported this recommendation to those projects' upstreams?

Simon McVittie @smcv · 2 years ago

Cinnamon: https://github.com/linuxmint/cinnamon/pull/9501

Michael Catanzaro @mcatanzaro · 2 years ago

I've contacted Christian (above) and Dodji (via email), who both agree it's time for libcroco to be archived.

I think that once we archive the repo, we probably won't be able to continue discussion in this issue report though, so we can wait a few days first, or even wait for it to happen naturally after a couple years.

Ray Strode @halfline · 2 years ago

fwiw, I had a quick look, and your patch and analysis in https://gitlab.gnome.org/GNOME/libcroco/-/issues/8#note_880221 seem right to me. I think if I were doing it, I would have been less surgical and just deployed a hammer that went over all calls, but your way seems right and fine.

I wonder though if you should do

```
cr_parser_push_error (a_this, ...)
```

explicitly so the reason why it fails is propagated?

Michael Catanzaro @mcatanzaro · 2 years ago

> I wonder though if you should do
>
> ```
> cr_parser_push_error (a_this, ...)
> ```
>
> explicitly so the reason why it fails is propagated?

I looked into this and I think the answer is probably: no, don't push an error, because the existing code uses either CHECK_PARSING_STATUS() or ENSURE_PARSING_COND() both inside these functions and after calling these functions. Those macros have counterparts CHECK_PARSING_STATUS_ERR() and ENSURE_PARSING_COND_ERR() that do the same thing but also call cr_parser_push_error(), and they're not being used here. Why not? I don't know. No clue. But since none of the other failure cases in these functions are using cr_parser_push_error(), and I don't see any obvious explanation of why that's used in some cases and not otherwise, seems best to match the surrounding code. do you agree?

Ray Strode @halfline · 2 years ago

so my take is it probably doesn't matter. If you don't specify a message, it's going to assign a generic one higher up the call chain. just thought it was a nice-to-have, doesn't seem critical.

Michael Catanzaro mentioned in issue Infrastructure/Infrastructure#392 (closed) 2 years ago

Michael Catanzaro mentioned in commit `federico/gnome-shell@fe66f58d` 2 years ago

Federico Mena Quintero mentioned in merge request GNOME/gnome-shell!1404 (merged) 2 years ago

Federico Mena Quintero @federico · 2 years ago

I've submitted this to GNOME/gnome-shell!1404 (merged), FWIW.

Michael Catanzaro mentioned in commit `federico/gnome-shell@44cbd1e7` 2 years ago

Federico Mena Quintero @federico · 2 years ago

Submitted this to the gettext maintainers via email.

Federico Mena Quintero @federico · 2 years ago

Submitted to Inkscape in https://gitlab.com/inkscape/inkscape/-/merge_requests/2202

Michael Catanzaro mentioned in commit `GNOME/gnome-shell@7b64eb28` 2 years ago

Andre Klapper @aklapper · 1 year ago

libcroco is not under development anymore and has been archived. This issue will not get fixed.

Andre Klapper closed 1 year ago

Please register or sign in to reply