New issue

Jump to bottom

API crashes #1769

Closed **Popvlvs** opened this issue on Sep 19 · 1 comment

Labels Bug

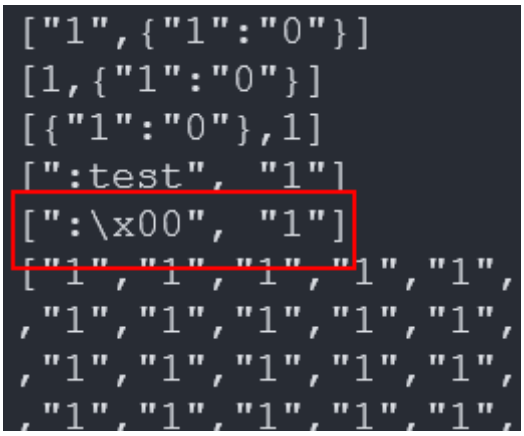
Popvlvs commented on Sep 19 • edited

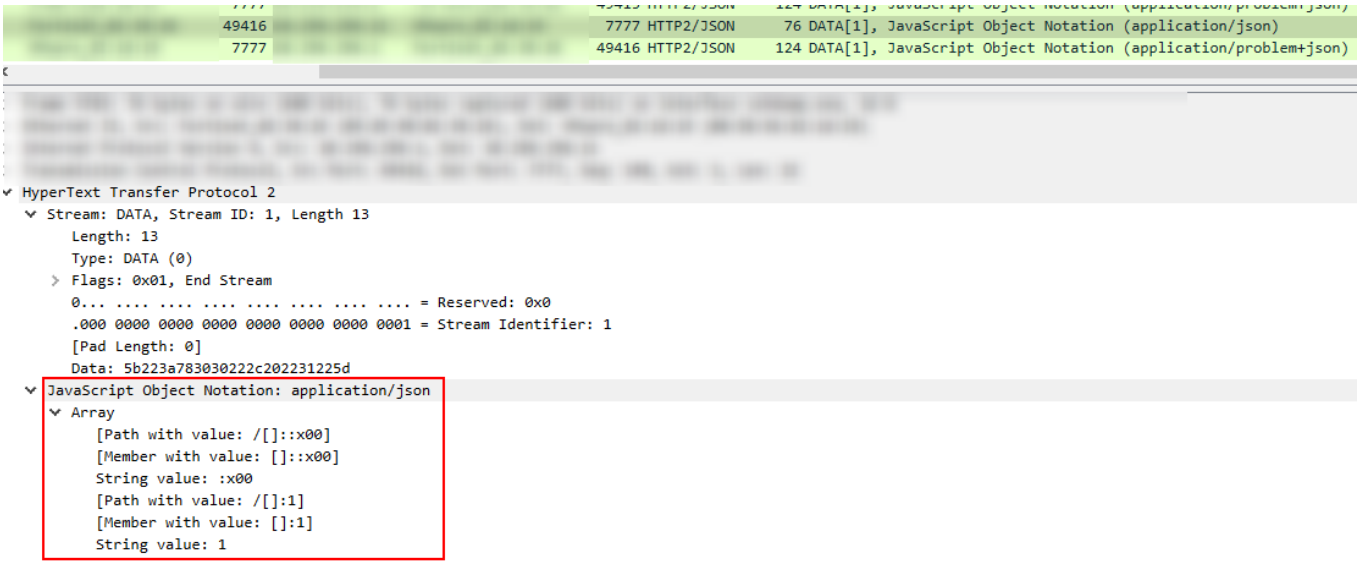
Hi,

I was fuzzing an AMF's API endpoint http://x.x.x.x:7777/namf-comm/v1/ue-contexts) with some random JSON payloads and it eventually crashed:

```
09/19 11:44:40.992: [sbi] ERROR: Unknown resource name [(null)] (../lib/sbi/message.c:1484)
09/19 11:44:40.992: [sbi] ERROR: parse_content() failed (../lib/sbi/message.c:559)
09/19 11:44:40.992: [amf] ERROR: cannot parse HTTP sbi_message (../src/amf/amf-sm.c:98)
09/19 11:44:41.083: [sbi] ERROR: Unknown resource name [(null)] (../lib/sbi/message.c:1484)
09/19 11:44:41.083: [sbi] ERROR: parse_content() failed (../lib/sbi/message.c:559)
09/19 11:44:41.083: [amf] ERROR: cannot parse HTTP sbi_message (../src/amf/amf-sm.c:98)
09/19 11:44:41.176: [sbi] ERROR: Unknown resource name [(null)] (../lib/sbi/message.c:1484)
09/19 11:44:41.176: [sbi] ERROR: parse_content() failed (../lib/sbi/message.c:559)
09/19 11:44:41.177: [amf] ERROR: cannot parse HTTP sbi_message (../src/amf/amf-sm.c:98)
09/19 11:44:41.266: [sbi] ERROR: Unknown resource name [(null)] (../lib/sbi/message.c:1484)
09/19 11:44:41.266: [sbi] ERROR: parse_content() failed (../lib/sbi/message.c:559)
09/19 11:44:41.266: [amf] ERROR: cannot parse HTTP sbi_message (../src/amf/amf-sm.c:98)
09/19 11:44:41.365: [sbi] ERROR: Overflow : Content-Length[6751], len[2704] (../lib/sbi/nghttp2-server.c:953)
09/19 11:44:41.365: [sbi] WARNING: on_data_chunk_recv: should not be reached. (../lib/sbi/nghttp2-server.c:955)
09/19 11:44:41.366: [core] FATAL: backtrace() returned 9 addresses (../lib/core/ogs-abort.c:37)
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogssbi.so.2(+0x29d3f) [0x7f1109c42d3f]
/lib/x86_64-linux-gnu/libnghttp2.so.14(nghttp2_session_mem_recv+0x101d) [0x7f110958236d]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogssbi.so.2(+0x27f35) [0x7f1109c40f35]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(+0x2aa09) [0x7f110a066a09]
/home/core5g/open5gs/install/bin/open5gs-amfd(+0x7d00) [0x5651b94efd00]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(+0x12639) [0x7f110a04e639]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x8609) [0x7f11097be609]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x43) [0x7f11096e3133]
```

It happens with NULL BYTE as a payload, as shown in the following pictures:





Regards

acetcom added a commit that referenced this issue on Sep 25

Fixed HTTP2 crashes for random JSON data (#1769) ✓ 724fa56

acetcom commented on Sep 25 Member

@Popvlvs

I've fixed it.

Thank you so much.
Sukchan

acetcom added the Bug label on Sep 25

Popvlvs closed this as completed on Sep 27

NLag added a commit to securitylab-repository/open5gs_ciot that referenced this issue on Oct 19

`Update repo to open5gs/open5gs main (#1)` ... `fdfe2c9`

Assignees

No one assigned

Labels

Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants