

[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 11:44:41.366: [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:

```
[ "1", { "1": "0" } ]  
[ 1, { "1": "0" } ]  
[ { "1": "0" }, 1 ]  
[ ":test", "1" ]  
[ ":\\x00", "1" ]  
[ "1", "1", "1", "1", "1", "  
    , "1", "1", "1", "1", "1", "  
    , "1", "1", "1", "1", "1", "  
    , "1", "1", "1", "1", "1"
```

7777	7777 HTTP/JSON	124 DATA[1], JavaScript Object Notation (application/json)
49416	7777 HTTP2/JSON	76 DATA[1], JavaScript Object Notation (application/json)
7777	49416 HTTP2/JSON	124 DATA[1], JavaScript Object Notation (application/problem+json)

1990-1991, 1991-1992, 1992-1993, 1993-1994, 1994-1995, 1995-1996, 1996-1997, 1997-1998, 1998-1999, 1999-2000, 2000-2001, 2001-2002, 2002-2003, 2003-2004, 2004-2005, 2005-2006, 2006-2007, 2007-2008, 2008-2009, 2009-2010, 2010-2011, 2011-2012, 2012-2013, 2013-2014, 2014-2015, 2015-2016, 2016-2017, 2017-2018, 2018-2019, 2019-2020, 2020-2021, 2021-2022, 2022-2023, 2023-2024, 2024-2025, 2025-2026, 2026-2027, 2027-2028, 2028-2029, 2029-2030, 2030-2031, 2031-2032, 2032-2033, 2033-2034, 2034-2035, 2035-2036, 2036-2037, 2037-2038, 2038-2039, 2039-2040, 2040-2041, 2041-2042, 2042-2043, 2043-2044, 2044-2045, 2045-2046, 2046-2047, 2047-2048, 2048-2049, 2049-2050, 2050-2051, 2051-2052, 2052-2053, 2053-2054, 2054-2055, 2055-2056, 2056-2057, 2057-2058, 2058-2059, 2059-2060, 2060-2061, 2061-2062, 2062-2063, 2063-2064, 2064-2065, 2065-2066, 2066-2067, 2067-2068, 2068-2069, 2069-2070, 2070-2071, 2071-2072, 2072-2073, 2073-2074, 2074-2075, 2075-2076, 2076-2077, 2077-2078, 2078-2079, 2079-2080, 2080-2081, 2081-2082, 2082-2083, 2083-2084, 2084-2085, 2085-2086, 2086-2087, 2087-2088, 2088-2089, 2089-2090, 2090-2091, 2091-2092, 2092-2093, 2093-2094, 2094-2095, 2095-2096, 2096-2097, 2097-2098, 2098-2099, 2099-2100, 2100-2101, 2101-2102, 2102-2103, 2103-2104, 2104-2105, 2105-2106, 2106-2107, 2107-2108, 2108-2109, 2109-2110, 2110-2111, 2111-2112, 2112-2113, 2113-2114, 2114-2115, 2115-2116, 2116-2117, 2117-2118, 2118-2119, 2119-2120, 2120-2121, 2121-2122, 2122-2123, 2123-2124, 2124-2125, 2125-2126, 2126-2127, 2127-2128, 2128-2129, 2129-2130, 2130-2131, 2131-2132, 2132-2133, 2133-2134, 2134-2135, 2135-2136, 2136-2137, 2137-2138, 2138-2139, 2139-2140, 2140-2141, 2141-2142, 2142-2143, 2143-2144, 2144-2145, 2145-2146, 2146-2147, 2147-2148, 2148-2149, 2149-2150, 2150-2151, 2151-2152, 2152-2153, 2153-2154, 2154-2155, 2155-2156, 2156-2157, 2157-2158, 2158-2159, 2159-2160, 2160-2161, 2161-2162, 2162-2163, 2163-2164, 2164-2165, 2165-2166, 2166-2167, 2167-2168, 2168-2169, 2169-2170, 2170-2171, 2171-2172, 2172-2173, 2173-2174, 2174-2175, 2175-2176, 2176-2177, 2177-2178, 2178-2179, 2179-2180, 2180-2181, 2181-2182, 2182-2183, 2183-2184, 2184-2185, 2185-2186, 2186-2187, 2187-2188, 2188-2189, 2189-2190, 2190-2191, 2191-2192, 2192-2193, 2193-2194, 2194-2195, 2195-2196, 2196-2197, 2197-2198, 2198-2199, 2199-2200, 2200-2201, 2201-2202, 2202-2203, 2203-2204, 2204-2205, 2205-2206, 2206-2207, 2207-2208, 2208-2209, 2209-2210, 2210-2211, 2211-2212, 2212-2213, 2213-2214, 2214-2215, 2215-2216, 2216-2217, 2217-2218, 2218-2219, 2219-2220, 2220-2221, 2221-2222, 2222-2223, 2223-2224, 2224-2225, 2225-2226, 2226-2227, 2227-2228, 2228-2229, 2229-2230, 2230-2231, 2231-2232, 2232-2233, 2233-2234, 2234-2235, 2235-2236, 2236-2237, 2237-2238, 2238-2239, 2239-2240, 2240-2241, 2241-2242, 2242-2243, 2243-2244, 2244-2245, 2245-2246, 2246-2247, 2247-2248, 2248-2249, 2249-2250, 2250-2251, 2251-2252, 2252-2253, 2253-2254, 2254-2255, 2255-2256, 2256-2257, 2257-2258, 2258-2259, 2259-2260, 2260-2261, 2261-2262, 2262-2263, 2263-2264, 2264-2265, 2265-2266, 2266-2267, 2267-2268, 2268-2269, 2269-2270, 2270-2271, 2271-2272, 2272-2273, 2273-2274, 2274-2275, 2275-2276, 2276-2277, 2277-2278, 2278-2279, 2279-2280, 2280-2281, 2281-2282, 2282-2283, 2283-2284, 2284-2285, 2285-2286, 2286-2287, 2287-2288, 2288-2289, 2289-2290, 2290-2291, 2291-2292, 2292-2293, 2293-2294, 2294-2295, 2295-2296, 2296-2297, 2297-2298, 2298-2299, 2299-2300, 2300-2301, 2301-2302, 2302-2303, 2303-2304, 2304-2305, 2305-2306, 2306-2307, 2307-2308, 2308-2309, 2309-2310, 2310-2311, 2311-2312, 2312-2313, 2313-2314, 2314-2315, 2315-2316, 2316-2317, 2317-2318, 2318-2319, 2319-2320, 2320-2321, 2321-2322, 2322-2323, 2323-2324, 2324-2325, 2325-2326, 2326-2327, 2327-2328, 2328-2329, 2329-2330, 2330-2331, 2331-2332, 2332-2333, 2333-2334, 2334-2335, 2335-2336, 2336-2337, 2337-2338, 2338-2339, 2339-2340, 2340-2341, 2341-2342, 2342-2343, 2343-2344, 2344-2345, 2345-2346, 2346-2347, 2347-2348, 2348-2349, 2349-2350, 2350-2351, 2351-2352, 2352-2353, 2353-2354, 2354-2355, 2355-2356, 2356-2357, 2357-2358, 2358-2359, 2359-2360, 2360-2361, 2361-2362,

```

✓ Hypertext Transfer Protocol 2
  ▾ Stream: DATA, Stream ID: 1, Length 13
    Length: 13
    Type: DATA (0)
    ▸ Flags: 0x01, End Stream
      0... .. = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0001 = Stream Identifier: 1
      [Pad Length: 0]
      Data: 5b223a783030222c202231225d
  ▾ JavaScript Object Notation: application/json
    ▾ Array
      [Path with value: /[:]:x00]
      [Member with value: [[:]:x00]
      String value: :x00
      [Path with value: /[:]:1]
      [Member with value: [[:]:1]
      String value: 1

```

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

 **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

