EmbedThis Appweb NPD Bug

May 9, 2021

EmbedThis Appweb NPD Bug

Summary

A npd bug in EmbedThis Appweb Community Edition **latest** Version 8.2.1 will lead to server crash.

> *Appweb and GoAhead are embedded web servers that are embedded in hundreds of millions of devices and applications. This includes printers, routers, switches, IP phones, mobile applications, data acquisition, military applications, WIFI gateways, factory automation, medical devices and many more.*

Analysis

The bug exists in `src/http/httpLib.c`

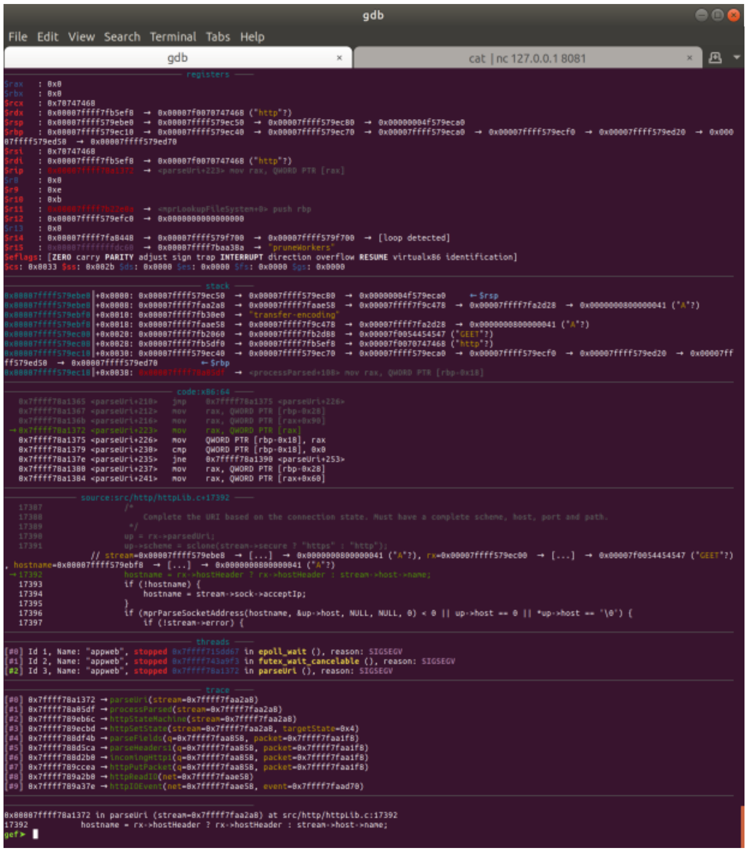
```
static void parseUri(HttpStream *stream)
    hostname = rx->hostHeader ? rx->hostHeader : stream->host->name;
```

When a HTTP request without a valid Host header is processed by the `parseUri()`, `rx->hostHeader` should be `0x00`, so `hostname = stream->host->name`.

However, `stream->host` is also `0x00`, thus `stream->host->name` will dereference a null pointer and the appweb process will crash due to segfault.

Reproduce

To reproduce this bug, build Appweb Community Edition Version 8.2.1 with make on a x64 Linux Distro, run the server with `./appweb --verbose . 127.0.0.1:8081`, and send the poc to it with `cat npd.txt | nc 127.0.0.1 8081`, and a segmentation fault should be expected.



```
──────────────────────────────────────── registers ────
$rax   : 0x0
$rbx   : 0x0
$rcx   : 0x70747468
$rdx   : 0x00007ffff7fb5ef8  →  0x00007f0070747468 ("http"?)
$rsp   : 0x00007ffff579ebe0  →  0x00007ffff579ec50  →  0x00007ffff579ec80  →  0x00000004f579eca0
$rbp   : 0x00007ffff579ec10  →  0x00007ffff579ec40  →  0x00007ffff579ec70  →  0x00007ffff579eca0  →  0x00007ffff579ecf0  →  0x00007ffff579ed20  →  0x000
07ffff579ed50  →  0x00007ffff579ed70
$rsi   : 0x70747468
$rdi   : 0x00007ffff7fb5ef8  →  0x00007f0070747468 ("http"?)
$rip   : 0x00007ffff78a1372  →  <parseUri+223> mov rax, QWORD PTR [rax]
$r8    : 0x0
$r9    : 0xe
$r10   : 0xb
$r11   : 0x00007ffff7b22e0a  →  <mprLookupFileSystem+0> push rbp
$r12   : 0x00007ffff579efc0  →  0x0000000000000000
$r13   : 0x0
$r14   : 0x00007ffff7fa8448  →  0x00007ffff579f700  →  0x00007ffff579f700  →  [loop detected]
$r15   : 0x00007fffffffdc60  →  0x00007ffff7baa38a  →  "pruneWorkers"
$eflags: [ZERO carry PARITY adjust sign trap INTERRUPT direction overflow RESUME virtualx86 identification]
$cs: 0x0033 $ss: 0x002b $ds: 0x0000 $es: 0x0000 $fs: 0x0000 $gs: 0x0000
──────────────────────────────────────────────────────────────────────
──────────────────────────────────────────── stack ────
0x00007ffff579ebe0│+0x0000: 0x00007ffff579ec50  →  0x00007ffff579ec80  →  0x00000004f579eca0     ← $rsp
0x00007ffff579ebe8│+0x0008: 0x00007ffff7faa2a8  →  0x00007ffff7faae58  →  0x00007ffff7f9c478  →  0x00007ffff7fa2d28  →  0x0000000800000041 ("A"?)
0x00007ffff579ebf0│+0x0010: 0x00007ffff7fb30e0  →  "transfer-encoding"
0x00007ffff579ebf8│+0x0018: 0x00007ffff7faae58  →  0x00007ffff7f9c478  →  0x00007ffff7fa2d28  →  0x0000000800000041 ("A"?)
0x00007ffff579ec00│+0x0020: 0x00007ffff7fb2060  →  0x00007ffff7fb2d88  →  0x00007f0054454547 ("GEET"?)
0x00007ffff579ec08│+0x0028: 0x00007ffff7fb5df0  →  0x00007ffff7fb5ef8  →  0x00007f0070747468 ("http"?)
0x00007ffff579ec10│+0x0030: 0x00007ffff579ec40  →  0x00007ffff579ec70  →  0x00007ffff579eca0  →  0x00007ffff579ecf0  →  0x00007ffff579ed20  →  0x00007ff
ff579ed50  →  0x00007ffff579ed70          ← $rbp
0x00007ffff579ec18│+0x0038: 0x00007ffff78a05df  →  <processParsed+108> mov rax, QWORD PTR [rbp-0x18]
──────────────────────────────────────────────────────────────────────
────────────────────────────────────── code:x86:64 ────
   0x7ffff78a1365 <parseUri+210>   jmp    0x7ffff78a1375 <parseUri+226>
   0x7ffff78a1367 <parseUri+212>   mov    rax, QWORD PTR [rbp-0x28]
   0x7ffff78a136b <parseUri+216>   mov    rax, QWORD PTR [rax+0x90]
 → 0x7ffff78a1372 <parseUri+223>   mov    rax, QWORD PTR [rax]
   0x7ffff78a1375 <parseUri+226>   mov    QWORD PTR [rbp-0x18], rax
   0x7ffff78a1379 <parseUri+230>   cmp    QWORD PTR [rbp-0x18], 0x0
   0x7ffff78a137e <parseUri+235>   jne    0x7ffff78a1390 <parseUri+253>
   0x7ffff78a1380 <parseUri+237>   mov    rax, QWORD PTR [rbp-0x28]
   0x7ffff78a1384 <parseUri+241>   mov    rax, QWORD PTR [rax+0x60]
──────────────────────────────────────────────────────────────────────
──────────────────────── source:src/http/httpLib.c+17392 ────
   17387                /*
   17388                    Complete the URI based on the connection state. Must have a complete scheme, host, port and path.
   17389                 */
   17390                up = rx->parsedUri;
   17391                up->scheme = sclone(stream->secure ? "https" : "http");
                   // stream=0x00007ffff579ebe8  →  [...]  →  0x0000000800000041 ("A"?), rx=0x00007ffff579ec00  →  [...]  →  0x00007f0054454547 ("GEET"?)
, hostname=0x00007ffff579ebf8  →  [...]  →  0x0000000800000041 ("A"?)
 → 17392                hostname = rx->hostHeader ? rx->hostHeader : stream->host->name;
   17393                if (!hostname) {
   17394                    hostname = stream->sock->acceptIp;
   17395                }
   17396                if (mprParseSocketAddress(hostname, &up->host, NULL, NULL, 0) < 0 || up->host == 0 || *up->host == '\0') {
   17397                    if (!stream->error) {
──────────────────────────────────────────────────────────────────────
────────────────────────────────────────── threads ────
[#0] Id 1, Name: "appweb", stopped 0x7ffff715dd67 in epoll_wait (), reason: SIGSEGV
[#1] Id 2, Name: "appweb", stopped 0x7ffff743a9f3 in futex_wait_cancelable (), reason: SIGSEGV
[#2] Id 3, Name: "appweb", stopped 0x7ffff78a1372 in parseUri (), reason: SIGSEGV
──────────────────────────────────────────────────────────────────────
──────────────────────────────────────────── trace ────
[#0] 0x7ffff78a1372 → parseUri(stream=0x7ffff7faa2a8)
[#1] 0x7ffff78a05df → processParsed(stream=0x7ffff7faa2a8)
[#2] 0x7ffff789eb6c → httpStateMachine(stream=0x7ffff7faa2a8)
[#3] 0x7ffff789ecbd → httpSetState(stream=0x7ffff7faa2a8, targetState=0x4)
[#4] 0x7ffff788df4b → parseFields(q=0x7ffff7faa858, packet=0x7ffff7faa1f8)
[#5] 0x7ffff788d5ca → parseHeaders1(q=0x7ffff7faa858, packet=0x7ffff7faa1f8)
[#6] 0x7ffff788d2b8 → incomingHttp1(q=0x7ffff7faa858, packet=0x7ffff7faa1f8)
[#7] 0x7ffff789ccea → httpPutPacket(q=0x7ffff7faa858, packet=0x7ffff7faa1f8)
[#8] 0x7ffff789a2b8 → httpReadIO(net=0x7ffff7faae58)
[#9] 0x7ffff789a37e → httpIOEvent(net=0x7ffff7faae58, event=0x7ffff7faad70)
──────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────

0x00007ffff78a1372 in parseUri (stream=0x7ffff7faa2a8) at src/http/httpLib.c:17392
17392           hostname = rx->hostHeader ? rx->hostHeader : stream->host->name;
gef➤ 
```