Issue 9904 - A Potential NPD

Status:	VERIFIED FIXED	**Reported:**	2022-08-24 11:20 UTC by 1157401338
		Modified:	2023-02-09 18:45 UTC (History)
Alias:	None	**CC List:**	0 users
Product:	OpenLDAP		
Component:	libraries (show other issues)	**See Also:**	
Version:	unspecified		
Hardware:	All All		
Importance:	--- normal		
Target Milestone:	2.5.14		
Assignee:	Howard Chu		
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments	
diagram of NPD (196.50 KB, image/jpeg) 2022-08-24 11:20 UTC, 1157401338	Details
Add an attachment (proposed patch, testcase, etc.)	

Note

You need to log in before you can comment on or make changes to this issue.

1157401338 2022-08-24 11:20:49 UTC Description

```
Created attachment 911 [details]
diagram of NPD

Hi, I found a NPD bug in the project source code of ldap, and I have shown the
execution sequence of the program that may have generated the bug on a
diagram,which is added to the attachment
The red text illustrates the steps that created the bug
the red arrows represent the call relationships
the file path can be seen in the blue framed section.

additionally,at step 4 I do not expand more detail about why function
ber_memalloc_x can return null(actually it can be seen as function malloc and the
reason ber_memalloc_x return null is same with malloc),because there are many code
snippet can be found in project source code that judge whether ber_memalloc_x
return null and make further process if return value equal to null.

I look forward to your reply and thank you very much for your patience!
```

Howard Chu 2022-08-24 13:44:05 UTC Comment 1

Thanks for the report. An image file was not necessary for explaining the issue.
Fixed in master.

1157401338 2022-08-25 03:56:55 UTC Comment 2

thank you for your effort.

similar potential bug of NPD can be found in
master/libraries/libldap/url.c,definition of function "ldap_url_parsehosts"

step1:
use strdup

step2:
assign return value to field ludp->lud_host at line 1399

step3:
derefer field ludp->lud_host in a call at 1432

code can be found in url
(https://git.openldap.org/openldap/openldap/-/blob/master/libraries/libldap/url.c#L1396-L1432)

Quanah Gibson-Mount 2022-08-25 15:57:42 UTC Comment 3

head:

- ea8dd2d2

by Howard Chu at 2022-08-24T14:40:51+01:00
ITS#9904 ldif_open_url: check for ber_strdup failure

RE26:

- c5c8c06a

by Howard Chu at 2022-08-24T18:22:42+00:00
ITS#9904 ldif_open_url: check for ber_strdup failure

RE25:

- 752d320c

by Howard Chu at 2022-08-24T18:23:50+00:00
ITS#9904 ldif_open_url: check for ber_strdup failure

Howard Chu 2022-08-25 16:03:52 UTC Comment 4

(In reply to 1157401338 from comment #2)
> thank you for your effort.
>
> similar potential bug of NPD can be found in
> master/libraries/libldap/url.c,definition of function "ldap_url_parsehosts"

Thanks, fixed in master. Note that this function is obsolete and the only
thing that uses it was deprecated long ago.

Quanah Gibson-Mount 2022-08-29 16:40:33 UTC Comment 5

head:
- 3f2abd0b

```
by Howard Chu at 2022-08-25T17:01:13+01:00
ITS#9904 ldap_url_parsehosts: check for strdup failure

RE26:

  • 840944e2
by Howard Chu at 2022-08-29T16:38:51+00:00
ITS#9904 ldap_url_parsehosts: check for strdup failure


RE25:

  • 6563fab9
by Howard Chu at 2022-08-29T16:39:49+00:00
ITS#9904 ldap_url_parsehosts: check for strdup failure
```

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