Issue 9202 - Should limit depth of nested filters

Status:	VERIFIED FIXED	**Reported:**	2020-04-06 00:14 UTC by Howard Chu
		Modified:	2021-09-11 10:13 UTC (History)
Alias:	None	**CC List:**	0 users
Product:	OpenLDAP		
Component:	slapd (show other issues)	**See Also:**	
Version:	unspecified		
Hardware:	All All		
Importance:	--- normal		
Target Milestone:	2.4.50		
Assignee:	OpenLDAP project		
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments	
fix (2.85 KB, patch) 2020-04-16 00:09 UTC, Howard Chu	Details
test program (1.27 KB, text/x-csrc) 2020-04-28 02:44 UTC, Ryan Tandy	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.

Howard Chu **2020-04-06 00:14:37 UTC** Description

```
The Samba team contacted us for input on a bug that's been reported to them;
an LDAP request with a very deeply nested filter (e.g. 10000 ORs) can cause
a stack overflow and crash their server.

https://bugzilla.samba.org/show_bug.cgi?id=14334

While this particular message doesn't crash slapd, it would be possible to
overflow slapd's stack using a message with over 38000 nested ORs. The message
with 10000 ORs is only 39KB, so our sockbuf_max_incoming limit doesn't
protect against it. We will patch slapd to limit the depth of nested
filters, and publish this bug concurrently with Samba team publishing theirs.
```

Howard Chu **2020-04-16 00:09:46 UTC** Comment 1

```
Created attachment 710 [details]
fix
```

Ryan Tandy **2020-04-16 01:04:05 UTC** Comment 2

I verified the issue and patch using ldapsearch:

```
ldapsearch -H ldap://:9000 -x -b dc=example,dc=com -LLL "$(python3 -c 'n=8000;
print("(|" * n + "(objectClass=*)" + ")" * n)')"
```

Quanah Gibson-Mount **2020-04-28 02:35:18 UTC** Comment 3

CVE-2020-10704

Ryan Tandy **2020-04-28 02:44:16 UTC** Comment 4

Created attachment 722 [details]
test program

Here's a better test program, not constrained by command line argument length limits.

Quanah Gibson-Mount **2020-04-28 14:02:21 UTC** Comment 6

master:
  • d38d48fc
by Howard Chu at 2020-04-28T13:58:15+00:00
ITS#9202 limit depth of nested filters

re24:

  • 98464c11
by Howard Chu at 2020-04-28T13:59:57+00:00
ITS#9202 limit depth of nested filters

Salvatore Bonaccorso **2020-04-28 16:59:12 UTC** Comment 7

(In reply to Quanah Gibson-Mount from comment #3)
> CVE-2020-10704

FWIW: Note that there is a dedicated CVE id for this issue in OpenLDAP, which is CVE-2020-12243.

Michael Ströder **2020-04-28 17:05:19 UTC** Comment 8

Please add the CVE-Id to CHANGES so downstream packagers take note of it.

Quanah Gibson-Mount **2020-04-28 17:20:19 UTC** Comment 9

(In reply to Michael Ströder from comment #8)
> Please add the CVE-Id to CHANGES so downstream packagers take note of it.

That's currently not a tracked item in the format of the CHANGES file.

I have been thinking of adding a customized field to bugzilla to track CVEs (we did that at a prior job I worked at).

We may want to consider a format change for RE25 to allow for CVEs in the CHANGES file as well.

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