Bug 1175568 - (CVE-2020-8027) VUL-0: CVE-2020-8027: openldap2: openldap_update_modules_path.sh starts daemons unconditionally and uses fixed paths in /tmp

Status: IN_PROGRESS

Classification: Novell Products
Product: SUSE Security Incidents
Component: Incidents
Version: unspecified
Hardware: Other Other

Priority: P3 - Medium **Severity**: Normal
Target Milestone: unspecified
Assigned To: Security Team bot
QA Contact: Security Team bot

URL: https://smash.suse.de/issue/266320/
Whiteboard: CVSSv3.1:SUSE:CVE-2020-8027:8.4:(AV:L...
Keywords:

Depends on: 1175683 1175685 ~~1175684~~
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-08-20 17:03 UTC by Thorsten Kukuk
Modified: 2020-10-27 00:40 UTC (History)
CC List: 8 users (show)

See Also:
Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Flags: matthias.gerstner: needinfo? (william.brown)

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.

Thorsten Kukuk 2020-08-20 17:03:29 UTC — Description

```
openldap_update_modules_path.sh from openldap2 has some critical problems:

1. it starts the slapd daemon on update unconditionally, even if it was not running
before and is not enabled. This can have really bad side effects, especially during
an offline upgrade with YaST2.

2. It uses fixed directories and files in /tmp without any checks if they already
exists. So the script would overwrite anything on the system if a user creates this
directories or files.
```

Matthias Gerstner 2020-08-24 08:52:12 UTC — Comment 1

```
This is a SUSE specific script that is part of the openldap2 package. It is run
once from a `%post` scriptlet in the package's spec file if a statefile in
/var/adm/openldap_modules_path_updated doesn't exist.

The script is found in Factory, the currently maintained openSUSE codestreams and
in the SUSE:SLE-15:Update codestream.

It looks pretty bad. It uses two fixed paths:

```
tmp_file='/tmp/ldap_conf_tmp.ldif'
backup='/tmp/slapd.d'
```

It doesn't call `set -o errexit`, thus failures to create e.g. `mkdir $backup`
aren't recognized.

Attack vectors are as follows:

1) /usr/sbin/slapcat -n0 -F ${conf_dir} -l ${tmp_file} -o ldif-wrap=no

This writes to $tmp_file, following symlinks. It is a DoS vector, content is not
directly under user control.

2) mkdir ${backup}
   cp -r ${conf_dir}/* ${backup}/

This will also follow symlinks, therefore whichever files are present in
${conf_dir} can be copied over to an arbitrary path, possibly overwriting existing
files of the same name.

Also the content of the configuration files will become accessible to an attacker,
which is not normally the case, because:

root# ls -lhd /etc/openldap/slapd.d/
drwxrwx--- 2 ldap ldap 4.0K 19. Aug 19:18 /etc/openldap/slapd.d/

3) /usr/sbin/slapadd -n0 -F ${conf_dir} -l ${tmp_file}

This will replace the existing slapd configuration by the possibly attacker
controlled file $tmp_file, therefore the slapd can be completely compromised.

4) /usr/bin/systemctl stop slapd.service
   /usr/bin/systemctl start slapd.service

This unconditional starting/stopping could prove problematic. The service should
only be started again if it was running in the first place. Also it would be better
not to stop a running service but find a runtime reconfiguration method, if
possible.
```

These findings should be treated under EMBARGO until updates are available. We will need to assign one or more CVEs. I'm not sure if one CVE suffices for "bad tmp file handling" or whether we should assign CVEs for issues 1) - 3)individually.

Issues 1) - 3) can be fixed by using `mktemp` instead of using the fixed paths.

Alexandros Toptsoglou 2020-09-22 15:09:31 UTC Comment 20

SLE15 is now released

Swamp Workflow Management 2020-09-22 19:24:15 UTC Comment 21

SUSE-SU-2020:2712-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1175568
CVE References: CVE-2020-8027
JIRA References:
Sources used:
SUSE Linux Enterprise Module for Legacy Software 15-SP2 (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise Module for Legacy Software 15-SP1 (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise Module for Development Tools 15-SP2 (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise Module for Development Tools 15-SP1 (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise Module for Basesystem 15-SP2 (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise Module for Basesystem 15-SP1 (src): openldap2-2.4.46-9.37.1

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 2020-09-26 04:14:36 UTC Comment 22

openSUSE-SU-2020:1534-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1175568
CVE References: CVE-2020-8027
JIRA References:
Sources used:
openSUSE Leap 15.1 (src): openldap2-2.4.46-lp151.10.18.1

Swamp Workflow Management 2020-09-26 10:17:24 UTC Comment 23

openSUSE-SU-2020:1539-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1175568
CVE References: CVE-2020-8027
JIRA References:
Sources used:
openSUSE Leap 15.2 (src): openldap2-2.4.46-lp152.14.9.1

Swamp Workflow Management 2020-10-22 19:17:05 UTC Comment 25

SUSE-SU-2020:2712-2: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1175568
CVE References: CVE-2020-8027
JIRA References:
Sources used:
SUSE Linux Enterprise Server for SAP 15 (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise Server 15-LTSS (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise High Performance Computing 15-LTSS (src): openldap2-2.4.46-9.37.1
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src): openldap2-2.4.46-9.37.1

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.

Matthias Gerstner 2020-10-23 11:23:04 UTC Comment 26

William, I'm seeing that in SLE-15-SP[12] you've replaced the original script by a new couple of scripts. Did you consider the backward compatibility and that it doesn't introduce any regressions for existing customers?

In Factory the fix is still missing. The embargo is lifted, however. Can you please also fix Factory now? And then please check whether the child bugs 1175683, 1175684 and 1175685 can be closed. Since you replaced the original script then they probably won't be applicable any more.

William Brown 2020-10-27 00:40:09 UTC Comment 27

(In reply to Matthias Gerstner from comment #26)

> William, I'm seeing that in SLE-15-SP[12] you've replaced the original
> script by a new couple of scripts. Did you consider the backward
> compatibility and that it doesn't introduce any regressions for existing
> customers?

Absolutely I considered that! I also did test the upgrade scenario and what it does. The script itself is only relevant for a subset of configs, and only for SLE12 to SLE15 upgrades.

>
> In Factory the fix is still missing. The embargo is lifted, however. Can you
> please also fix Factory now? And then please check whether the child bugs
> 1175683, 1175684 and 1175685 can be closed. Since you replaced the original
> script then they probably won't be applicable any more.

Done, I am submitting now.
