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

Bug 1200885 - (CVE-2022-31250) VUL-0: CVE-2022-31250: keylime: %post scriplet allows for privilege escalation from keylime user to root

Status:	NEW
Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Incidents
Version:	unspecified
Hardware:	Other openSUSE Tumbleweed
Priority:	P3 - Medium **Severity**: Normal
Target Milestone:	---
Assigned To:	Alberto Planas Dominguez
QA Contact:	Security Team bot
URL:	https://smash.suse.de/issue/335343/
Whiteboard:	CVSSv3.1:SUSE:CVE-2022-31250:7.8:(AV:...
Keywords:	
Depends on:	
Blocks:	
	Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2022-06-23 14:38 UTC by Johannes Segitz
Modified:	2022-08-03 22:20 UTC (History)
CC List:	2 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 2022-06-23 14:38:24 UTC Description

```
Problematic section:

%post -n %{srcname}-tpm_cert_store
# Help the upgrade process when moving to a non-root services
chown -R keylime:tss %{_sharedstatedir}/%{srcname}/ca 2> /dev/null || :
chown -R keylime:tss %{_sharedstatedir}/%{srcname}/secure 2> /dev/null || :
chown -R keylime:tss %{_sharedstatedir}/%{srcname}/cv_ca 2> /dev/null || :
chown keylime:tss %{_sharedstatedir}/%{srcname}/*.sqlite 2> /dev/null || :
chown keylime:tss %{_sharedstatedir}/%{srcname}/*.yml 2> /dev/null || :
chown keylime:tss %{_sysconfdir}/%{srcname}.conf 2> /dev/null || :
```

```
This allows the keylime user to escalate to root as %{_sharedstatedir}/%{srcname}
is owned by keylime. POC:
sh-5.1$ pwd
/var/lib/keylime
sh-5.1$ id
uid=446(keylime) gid=446(keylime) groups=446(keylime)
context=unconfined_u:unconfined_r:unconfined_t:s0
sh-5.1$ ln -s /etc/passwd passwd.sqlite
sh-5.1$ ls -l
total 4
lrwxrwxrwx. 1 keylime keylime   11 Jun 23 16:27 passwd.sqlite -> /etc/passwd
drwxr-xr-x. 2 root    root    4096 Jun 23 16:23 tpm_cert_store

as root simulate a package update with
zypper in -f keylime-tpm_cert_store

After that /etc/passwd is owned by keylime
-rw-r--r--. 1 keylime tss 3733 Jun 23 16:23 /etc/passwd
```

Please remove the chown calls. In general it's not safe to do this if unprivileged users can influence parts of the path where the operation is done

Johannes Segitz 2022-06-23 14:41:58 UTC Comment 1

This is an embargoed bug. This means that this information is not public.

Please do NOT:
- talk to other people about this unless they're involved in fixing the issue
- make this bug public
- submit this into OBS (e.g. fix Leap/Tumbleweed) until this bug becomes public. This means that the security team removed the EMBARGOED tag from the bug title after we verified that there's already information about this bug publicly available. If you find such information yourself and the bug is still embargoed please contact us

Your primary responsibility is to apply a fix for this issue.
Here is some guidance on openSUSE package maintenance:
- https://en.opensuse.org/openSUSE:Package_maintenance
- https://en.opensuse.org/openSUSE:Maintenance_update_process

You need to submit AFTER the bug became public, to the current openSUSE Leap codestreams, and to the devel project of your package.

The security team will then take the following steps:
- We wait for your submission and package them into an incident for QA testing. The QA tester might reach out to you if they find issues with the update.
- If QA doesn't find any issues, we publish the updates.

You can contact us at:

* IRC: irc.suse.de #security
* Do NOT use Slack or any non-SUSE hosted messaging services
* Email: security-team@suse.de

Johannes Segitz 2022-06-23 14:42:30 UTC Comment 2

Internal CRD: 2022-07-25 or earlier

Alberto Planas Dominguez 2022-06-23 14:58:46 UTC Comment 3

(In reply to Johannes Segitz from comment #0)

> Please remove the chown calls. In general it's not safe to do this if
> unprivileged users can influence parts of the path where the operation is
> done

Done in SR#984735.

Those calls are there because now the different services was executed as root, creating some directories as root in the process. Now we implemented a user downgrade mechanism, so the different services are running under a non privilege user (keylime). The %post code was put there to change the user to this keylime one, so the new agents can still write on it after the upgrade.

Is there a way that I can still change the owner of those files and directories in a way that do not produce any security issue?

Alberto Planas Dominguez 2022-06-23 16:13:56 UTC Comment 4

Guianluca Grabrielli pinged me that I make the mistake of releasing the fix.

Alberto Planas Dominguez 2022-06-23 16:15:01 UTC Comment 5

Remove EMBARGOED tag after talking with Johannes Segitz.

Matthias Gerstner 2022-07-04 08:12:08 UTC Comment 7

(In reply to aplanas@suse.com from comment #3)

> Is there a way that I can still change the owner of those files and
> directories in a way that do not produce any security issue?

It is pretty difficult in shell code. If is just one level below a user controlled directory then `chown -h` suffices. If it is deeper below a user controlled directory then you can use sequences like (in bash):

```
    cd -P /some/user/controlled/dir
    if [ "$PWD" != "/some/user/controlled/dir" ]; then
        echo "followed symlink"
        exit 1
    else
        chown -h someuser somefile
    fi
```

Alberto Planas Dominguez 2022-07-14 08:46:36 UTC Comment 8

Thanks all for the help. As the SR showed I removed the code from TW, but to fix an issue in SLE I reintroduced a version of it:

For files I am doing this:

```
chown -h keylime:tss /filename/path 2> /dev/null || :
```

I checked that this is indeed doing the correct thing: change the ownership of the link itself, but not the linked file.

For directories I am doing this:

```
chown -h -R keylime:tss /directory/path 2> /dev/null || :
```

I checked this adding file links inside the directory, links to directories inside the directory and converting the directory in a link itself. In all the three tests I saw that it is doing the right thing: change the ownership of the link itself, and never of the linked element. For linked directories I also checked that is not walking it neither.

The code is https://build.suse.de/package/view_file/home:aplanas:branches:SUSE:SLE-15-SP4:Update/keylime/keylime.spec?expand=1, and if there are no complains I will do a MU soon.

I hope that this does not re-introduce a variant of this CVE.

Swamp Workflow Management 2022-08-03 22:20:45 UTC Comment 12

SUSE-SU-2022:2658-1: An update that solves two vulnerabilities and has two fixes is now available.

Category: security (important)
Bug References: 1199253,1200885,1201466,1201866
CVE References: CVE-2022-1053,CVE-2022-31250
JIRA References:
Sources used:
openSUSE Leap 15.4 (src):   keylime-6.3.2-150400.4.11.1
SUSE Linux Enterprise Module for Basesystem 15-SP4 (src):   keylime-6.3.2-150400.4.11.1

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.

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

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