Bug 1164472 - (CVE-2020-24330) VUL-0: CVE-2020-24330: trousers: TrouSerS tcsd privilege escalation tss to root user

Status: IN_PROGRESS

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

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

URL: https://smash.suse.de/issue/253422/
Whiteboard: CVSSv3.1:SUSE:CVE-2020-24330:7.8:(AV:...
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-02-20 12:00 UTC by Matthias Gerstner
Modified: 2022-08-12 19:19 UTC (History)
CC List: 4 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.

Matthias Gerstner 2020-02-20 12:00:59 UTC Description

I stumbled across the tcsd in the trousers tpm 1.2 package no handling the user privilege drop to the 'tss' user well. I've sent the following email to the upstream contact that is noted in trouser's README file as a security contact:

```
Hi,

I'm contacting you, because your email is listed in the TrouSerS README
[1] as a contact for security issues in TrouSerS.

I want to report a couple of security related findings in TrouSerS.  I
noticed that the tcsd daemon in TrouSerS is dropping root privileges too
late in the startup process and does so also incompletely:

1) TrouSerS upstream recommends the state directory /var/lib/tpm to be
   owned by the unprivileged user tss:tss, mode 0700. However, the tcsd
   daemon when started as root drops to user tss too late. As root the
   daemon creates at least the following file in the state directory
   (taken from strace output):

   openat(AT_FDCWD, "/var/lib/tpm/system.data", O_RDWR|O_CREAT, 0600) = 4

   This means a compromised tss user account can prepare a symlink
   attack in this path, causing arbitrary paths to be
   created/overwritten in the system. This is at least a local
   denial-of-service attack vector.

2) tcsd only drops the root user id via `setuid()` but not the root
   group id. Therefore tcsd continues to run with root group privileges.
   Should the daemon be compromised then the root group privileges can
   be used to extend privileges beyond what the tcsd actually needs to
   have.

3) Furthermore the spec file example [2] in the trousers repository is
   not using safe file and directory modes:

   ```
   %post
   # create the default location for the persistent store files
   if test -e %{_localstatedir}/tpm; then
        mkdir -p %{_localstatedir}/tpm
        /bin/chown tss:tss %{_localstatedir}/tpm
        /bin/chmod 1777 %{_localstatedir}/tpm
   fi

   # chown the daemon
   /bin/chown tss:tss %{_sbindir}/tcsd
   ```

   The localstatedir being world-readable and carrying a sticky bit
   doesn't make much sense. It also fosters further symlink attacks
   available to all users. Furthermore it might present an information
   leak depending on the data stored e.g. in /var/lib/tpm/system.data.

   The `chown tss:tss /usr/sbin/tcsd` would allow a local root exploit,
   because it allows the tss user to replace this program by a different
   one, which will then potentially be run by the root user.

I've been looking in a couple of distributions and I found out the
following:

- Debian and Gentoo are not affected by 1), 2) since they use init
  scripts with start-stop-daemon and run tscd directly as the tss user.

- SUSE and Fedora/RedHat use systemd units to start tcsd as root and
```

rely on the daemon to drop privileges accordingly. Therefore they are affected by 1), 2).

As a quick protection measure I recommend to run tcsd directly as the tss user via systemd or init scripts and thus don't rely on the tscd privilege drop logic. This should only require appropriate permissions for /var/lib/tpm and the /dev/tpm0 device (via e.g. udev rules) to work.

To fix the TrouSerS code I recommend to either:

a) remove the privilege drop code completely, refuse running as root and require the daemon always to be run as the tss user

or

b) move the privilege drop code into an earlier stage of the daemon code, before any files are written, and to also drop the root gid to the tss gid.

At SUSE we follow a security disclosure policy [3] that allows the issue to remain private for up to 90 days. Please inform me whether you can confirm the findings described above and how long you want to keep it private, if at all. Also please tell me whether you want to assign CVE identifiers for the individual findings, and how you intend to handle the further disclosure process.

Thank you

Matthias

[1]: https://sourceforge.net/p/trousers/trousers/ci/master/tree/README
[2]: https://sourceforge.net/p/trousers/trousers/ci/master/tree/dist/trousers.spec.in
[3]: https://en.opensuse.org/openSUSE:Security_disclosure_policy
```

This bug here is mostly about item 1) which clearly deserves a CVE. item 2) is closely related, could use its separate bug and CVE. Since with 2) a compromised tss account can still cause symlink attacks for files where the root group has write permission. 3) is more a cosmetical kind of thing, I hope. Not used in SUSE packages this way anyways.

I communicated the security policy to upstream therefore tracking the latest CRD here accordingly:

CRD: 2020-05-19 or earlier

---

**Matthias Gerstner** 2020-04-02 08:04:36 UTC Comment 1

As it turned out the security contact address in the upstream README was wrong. I tried the regular maintainer debora@linux.ibm.com instead. From her I've got a reply on 2020-03-16. She wants to look into it but since then nothing new.

---

**Matthias Gerstner** 2020-05-20 08:41:25 UTC Comment 2

So this issue is going to be published now without support from upstream since there is no reply. I will first try to fix our own packaging. We can't pull a CVE at the moment, because IBM is a CNA themselves. If they don't react even after publication then we can still approach Mitre to get one ourselves.

---

**Matthias Gerstner** 2020-05-20 08:52:47 UTC Comment 3

In the current upstream code in src/tcsd/svrside.c:458 (main function) is a call to `tcsd_startup()` where the vulnerable code is called. The privilege drop of the uid is only done later in src/tcsd/svrside.c:476.

`ps_dirs_init()` checks the `system_ps_dir` (/var/lib/tpm), tries to create it with mode 0700 but does not `chown()` it. If it already exists then it also tries to correct the mode to 0700. This conflicts with our packaging where the mode is set to 0770.

In `ps_init_disk_cache()` the `get_file()` function triggers the open of /var/lib/tpm/system.data with `O_CREAT | O_RDWR`.

To fix this in Factory I'll take the route to start tcsd as the tss user right away. This reduces any risks that might still lurk in the code, because the startup sequence and privilege drop logic seem pretty inconsistent to me, security wise. This also requires a udev rules file to be shipped, however, because currently tcsd opens /dev/tpm0 as root before dropping to the tss uid. It also requires changing the ownership of a possible already existing /var/lib/tpm/system.data to tss.

For backporting to older codestreams I consider adding `O_NOFOLLOW` to the `open()` in `get_file()` and also to additionally drop the gid after initialization.

---

**Matthias Gerstner** 2020-05-20 10:16:21 UTC Comment 4

The situation is getting worse the more I'm looking into it. It turns out that the /etc/tcsd.conf file MUST be owned by tss:tss mode 600. In this config paths to kernel files as well as to the system_ps_file are defined:

```
 root # grep system_ps_file /etc/tcsd.conf
 # Option: system_ps_file
 # system_ps_file = /var/lib/tpm/system.data
```

This means the unprivileged tss user can not only stage a symlink attack in /var/lib/tpm, but it can also change the path where the tcsd is trying to create /var/lib/tpm with mode 0700. Luckily the code isn't `chown()`'ing this path to the tss user, otherwise we'd have a full tss to root privilege escalation.

There might be more attack vectors through the config file like information leaks.

A fix needs to change the mode and ownership of /etc/tcsd.conf to root:tss 0640. There's no need for the tss user to write to this config file.

OBSbugzilla Bot 2020-05-20 11:40:07 UTC Comment 5

This is an autogenerated message for OBS integration:
This bug (1164472) was mentioned in
https://build.opensuse.org/request/show/807580 Factory / trousers

---
```

Swamp Workflow Management 2020-05-26 19:13:11 UTC Comment 8

```
SUSE-RU-2020:1483-1: An update that has one recommended fix can now be installed.

Category: recommended (important)
Bug References: 1164472
CVE References:
Sources used:
SUSE Linux Enterprise Module for Basesystem 15-SP1 (src):    trousers-0.3.14-6.6.2

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 2020-05-26 19:18:05 UTC Comment 9

```
SUSE-RU-2020:1484-1: An update that has one recommended fix can now be installed.

Category: recommended (important)
Bug References: 1164472
CVE References:
Sources used:
SUSE OpenStack Cloud Crowbar 8 (src):    trousers-0.3.14-3.3.1
SUSE OpenStack Cloud 8 (src):    trousers-0.3.14-3.3.1
SUSE Linux Enterprise Software Development Kit 12-SP5 (src):    trousers-0.3.14-
3.3.1
SUSE Linux Enterprise Software Development Kit 12-SP4 (src):    trousers-0.3.14-
3.3.1
SUSE Linux Enterprise Server for SAP 12-SP3 (src):    trousers-0.3.14-3.3.1
SUSE Linux Enterprise Server 12-SP5 (src):    trousers-0.3.14-3.3.1
SUSE Linux Enterprise Server 12-SP4 (src):    trousers-0.3.14-3.3.1
SUSE Linux Enterprise Server 12-SP3-LTSS (src):    trousers-0.3.14-3.3.1
SUSE Linux Enterprise Server 12-SP3-BCL (src):    trousers-0.3.14-3.3.1
SUSE Enterprise Storage 5 (src):    trousers-0.3.14-3.3.1
HPE Helion Openstack 8 (src):    trousers-0.3.14-3.3.1

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 2020-06-02 07:12:56 UTC Comment 10

```
openSUSE-RU-2020:0755-1: An update that has one recommended fix can now be
installed.

Category: recommended (important)
Bug References: 1164472
CVE References:
Sources used:
openSUSE Leap 15.1 (src):    trousers-0.3.14-lp151.4.7.1
```

Matthias Gerstner 2020-06-08 07:56:03 UTC Comment 11

```
All updates are submitted. Reassigning to reactive security.
```

Alexander Bergmann 2020-08-14 06:49:17 UTC Comment 12

```
CVE-2020-24330 was assigned to this bug.

References:
https://nvd.nist.gov/vuln/detail/CVE-2020-24330
```

Alexander Bergmann 2020-08-17 07:52:44 UTC Comment 13

```
Three CVEs got assigned to this issue:

- CVE-2020-24330: tcsd daemon is started with root privileges instead of by the tss
user, it fails to drop the root gid privilege when no longer needed.
- CVE-2020-24331: The tss user still has read and write access to the
/etc/tcsd.conf file (which contains various settings related to this daemon).
- CVE-2020-24332: The creation of the system.data file is prone to symlink attacks.
The tss user can be used to create or corrupt existing files, which could possibly
lead to a DoS attack.
```

Thomas Leroy 2022-08-09 09:51:38 UTC Comment 14

```
Hi Matthias, it seems that we still have the following codestreams affected
- SUSE:SLE-11-SP3:Update
- SUSE:SLE-12:Update
- SUSE:SLE-15:Update

Can it be possible to submit a fix for these three? :)
```

Matthias Gerstner 2022-08-10 08:05:52 UTC Comment 17

```
(In reply to Thomas Leroy from comment #14)
> Hi Matthias, it seems that we still have the following codestreams affected
> - SUSE:SLE-11-SP3:Update
> - SUSE:SLE-12:Update
> - SUSE:SLE-15:Update
>
> Can it be possible to submit a fix for these three? :)

I submitted updates for these three codestreams. It was not all that easy for the
old codestreams but hopefully everything works out.
```

Thomas Leroy 2022-08-10 08:06:46 UTC Comment 18

```
(In reply to Matthias Gerstner from comment #17)
> (In reply to Thomas Leroy from comment #14)
> > Hi Matthias, it seems that we still have the following codestreams affected
> > - SUSE:SLE-11-SP3:Update
> > - SUSE:SLE-12:Update
> > - SUSE:SLE-15:Update
> >
> > Can it be possible to submit a fix for these three? :)
```

>
> I submitted updates for these three codestreams. It was not all that easy
> for the old codestreams but hopefully everything works out.

Thanks a lot Matthias!

Swamp Workflow Management 2022-08-12 19:15:39 UTC Comment 19

SUSE-SU-2022:2798-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1164472
CVE References: CVE-2020-24330
JIRA References:
Sources used:
SUSE Linux Enterprise Server for SAP 15 (src): trousers-0.3.14-150000.3.3.1
SUSE Linux Enterprise Server 15-LTSS (src): trousers-0.3.14-150000.3.3.1
SUSE Linux Enterprise High Performance Computing 15-LTSS (src): trousers-0.3.14-150000.3.3.1
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src): trousers-0.3.14-150000.3.3.1

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 2022-08-12 19:19:04 UTC Comment 20

SUSE-SU-2022:2800-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1164472
CVE References: CVE-2020-24330
JIRA References:
Sources used:
SUSE Linux Enterprise Server 12-SP2-BCL (src): trousers-0.3.13-3.3.1

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.
