Hash Suite - Windows password security audit tool. GUI, reports in PDF.

Date: Fri, 14 Aug 2020 01:39:34 -0700
From: Debora Velarde Babb <debora@...ux.ibm.com>
To: Matthias Gerstner <mgerstner@...e.de>, oss-security@...ts.openwall.com
Cc: trousers-tech@...ts.sourceforge.net, security <security@...e.de>
Subject: Re: [TrouSerS-tech] Multiple Security Issues in the TrouSerS tpm1.2
 tscd Daemon

On Wed, 2020-05-20 at 14:54 +0200, Matthias Gerstner wrote:
>
>
> Security Issues
> ===============
>
> The security issues resulting from this are as follows:
>
> a) Since /var/lib/tpm is owned by the tss user (as per
> dist/Makefile.am), the
>   creation of the `system.data` file in step 3) is prone to symlink
> attacks. The
>   tss user can thereby cause the creation of new files or the
> corruption of
>   existing files. These new files end up with mode 0600 and no
> `chown()` to the
>   tss user is performed by the tcsd. Thus it looks like no full
> local root
>   privilege escalation can be achieved but only DoS attacks.

CVE-2020-24332 is assigned to issue a)

[Suggested description]
An issue was discovered in TrouSerS through 0.3.14.
If the tcsd daemon is started with root privileges, 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.

>
> b) The tcsd only drops the root uid, not the root gid in step 4). A
> call to
>   `setgid()` is missing. Therefore the tcsd continues to run with
> root group
>   privileges it doesn't actually require. This could allow further
> privilege
>   escalations when combined with other, yet unknown attack vectors.

CVE-2020-24330 assigned to security issue b)

[Suggested description]
An issue was discovered in TrouSerS through 0.3.14.
If the 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.

>
> c) The configuration file /etc/tcsd.conf is _required_ by the tcsd to
> be
>   owned by tss:tss mode 0600. Therefore the unprivileged user can
> change all
>   daemon related settings, including the `system_ps_file` path. This
> means
>   the `mkdir()` and `chmod()` performed in step 2) can be directed
> to an
>   arbitrary path. This also includes the symlink attack described in
> a)
>   for arbitrary paths.
>
>   Further security issues could stem from this by manipulating other
> config
>   file options. I did not look deeper into this.

CVE-2020-24331 is assigned to security issue c)

[Suggested description]
An issue was discovered in TrouSerS through 0.3.14.
If the tcsd daemon is started with root privileges, the tss user still
has read and write access to the /etc/tcsd.conf file (which contains
various settings related to this daemon).

>
> d) Not directly related to the logic above. The example RPM spec file
> [5] in
>   the TrouSerS repository is using unsafe file and directory modes
> for
>   /var/lib/tpm and /usr/sbin/tcsd:
>
>    ```
>    # 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
>    ```
>
>   So here a public sticky-bit directory is setup in /var/lib/tpm.
> This could
>   allow arbitrary users to setup the symlink attack mentioned in a).
> It could
>   also lead to an information leak. Once the tcsd is started as root
> the mode
>   of /var/lib/tpm will be corrected in step 1), however.
>
>   Passing ownership of /usr/sbin/tcsd to the tss user would allow
> the tss
>   user to replace the tcsd binary by malicious code that will
> potentially be
>   executed by the root user, leading to arbitrary code execution.
>
>   I'm not aware of any distribution actually using this spec file or
> parts of
>   it. Still it is a very bad example.
>
> Mitigation and Bugfixes
> =======================
>
> It seems best to me to run the tcsd as the tss:tss user and group
> right away
> and to not rely on the privilege drop logic implemented in the daemon
> itself.
> All of a), b) and c) should no longer be problematic in this case. I
> found
> that on Debian and Gentoo Linux this is already the case. To make
> this work a
> udev rule needs to be packaged that passes ownership of /dev/tpm0
> device to

> the tss user. To prevent regressions when switching from the
> privilege drop
> approach to this new approach, a possibly already existing
> /var/lib/tpm/system.auth file needs to be safely chown()'ed to the
> tss user
> during package updates.
>
> On SUSE and Fedora Linux the tcsd is started as root via systemd,
> thus they
> are affected by the security issues. A preliminary suggested source
> code fix
> is attached to this mail. It makes sure that `O_NOFOLLOW` is added to
> step 3)
> to prevent a symlink attack. It also adds a drop of the root gid to
> the tss
> gid. And it modifies the check of /etc/tcsd.conf such that ownership
> root:tss
> and mode 0640 are necessary. The packaging needs to be adjusted
> accordingly.
>
> The correct long term fix should probably be to *only* open /dev/tpm0
> as root,
> immediately drop to tss:tss and only then perform the further
> initialization
> steps. The initialization sequence in `tcsd_startup()` is currently
> running
> completely in the root user context and seems rather complex. Maybe
> there are
> more details to this that I don't know of yet. For this reason I
> didn't try a
> patch in this direction yet.
>
> Upstream Reporting
> ==================
>
> I reported issues a), b) and d) privately to the documented upstream
> contacts
> without much success (see Timeline below). The SUSE Security Team 90
> days
> maximum disclosure time has been reached, therefore I'm publishing
> this now in
> an uncoordinated way. While working on a fix I additionally
> discovered issue
> c). SUSE is tracking the issues in bsc#1164472 [6] currently.
>
> Issues a), b) and c) deserve CVE assignments in my opinion. I can't
> request
> CVEs myself though, because IBM upstream is a CNA themselves.
> Therefore
> upstream is required to assign their own CVEs.
>
> Timeline
> ========
>
> 2020-02-19: I reported findings a), b) and d) to
> honclo@...ux.vnet.ibm.com,
>   the security contact of the project according to the
> README file [2].
> 2020-02-28: I reported findings a), b) and d) to debora@...ux.ibm.com
> , the
>   maintainer of the project according to the AUTHORS file
> [3].
> 2020-03-16: I received a reply from debora@...ux.ibm.com, stating
> that she
>   will look into the findings.
> 2020-05-06: I reminded debora@...ux.ibm.com that the latest
> disclosure time
>   [4] for the findings is approaching and asked for any
> updates.
> 2020-05-20: I started working on a bugfix and mitigations, discovered
> the
>   additional finding c) and started publishing the
> findings.
>
> [1]: https://sourceforge.net/projects/trousers
> [2]:
> https://sourceforge.net/p/trousers/trousers/ci/master/tree/README
> [3]:
> https://sourceforge.net/p/trousers/trousers/ci/master/tree/AUTHORS
> [4]: https://en.opensuse.org/openSUSE:Security_disclosure_policy
> [5]:
> https://sourceforge.net/p/trousers/trousers/ci/master/tree/dist/trousers.spec.in
> [6]: https://bugzilla.suse.com/show_bug.cgi?id=1164472
>
> Best Regards
>
> Matthias
>
> _____
> TrouSerS-tech mailing list
> TrouSerS-tech@...ts.sourceforge.net
> https://lists.sourceforge.net/lists/listinfo/trousers-tech

Powered by blists - more mailing lists

Please check out the Open Source Software Security Wiki, which is counterpart to this mailing list.

Confused about mailing lists and their use? Read about mailing lists on Wikipedia and check out these guidelines on proper formatting of your messages.