Bug 1171883 - (CVE-2020-8025) VUL-0: CVE-2020-8025: pcp: outdated entries in permissions profiles for /var/lib/pcp/tmp/* may cause security issues

Status: IN_PROGRESS

Classification: openSUSE
Product: openSUSE Tumbleweed
Component: Security
Version: Current
Hardware: Other Other

Priority: P3 - Medium **Severity**: Normal (vote)
Target Milestone: ---
Assigned To: Security Team bot
QA Contact: E-mail List

URL: https://smash.suse.de/issue/259623/
Whiteboard: CVSSv3.1:SUSE:CVE-2020-8025:6.1:(AV:L...
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-05-19 13:13 UTC by Matthias Gerstner
Modified: 2022-05-27 19:16 UTC (History)
CC List: 11 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 2020-05-19 13:13:34 UTC — Description

```
The security team is currently sanity checking the profiles in the
Base:System/permissions package. While doing so we noticed the following
issues with entries related to the pcp package:

The following paths are no longer part of the package:

- /var/lib/pcp/tmp/pmdabash
- /var/lib/pcp/tmp/mmv

Have last been seen in openSUSE-Leap-42.2 in package
pcp-3.6.10-8.25.x86_64.rpm.

The following paths have no corresponding %set_permissions and
%verify_permissions invocation in the package's spec file:

- /var/lib/pcp/tmp
- /var/lib/pcp/tmp/pmie
- /var/lib/pcp/tmp/pmlogger

These paths have the following settings the permissions package's profiles:

permissions.easy:       /var/lib/pcp/tmp/               root:root         1777
permissions.easy:       /var/lib/pcp/tmp/pmlogger/      root:root         1777
permissions.easy:       /var/lib/pcp/tmp/pmie/          root:root         1777

permissions.secure:     /var/lib/pcp/tmp/               root:root         0755
permissions.secure:     /var/lib/pcp/tmp/pmlogger/      root:root         0755
permissions.secure:     /var/lib/pcp/tmp/pmie/          root:root         0755

permissions.paranoid:   /var/lib/pcp/tmp/               root:root         0755
permissions.paranoid:   /var/lib/pcp/tmp/pmlogger/      root:root         0755
permissions.paranoid:   /var/lib/pcp/tmp/pmie/          root:root         0755

The invocation of %set_permissions and %verify_permissions was removed in the
Factory package in revision 36 when a dedicated user and group 'pcp:pcp' have
been introduced for the directories listed above.
```

Matthias Gerstner 2020-05-19 13:23:06 UTC — Comment 1

```
This issue is a possible security problem, because although the package is no
longer calling %set_permissions and %verify_permissions, whenever the `ckstat`
tool is called (this is done sooner or later through other package
installations), the permissions from the profiles will apply.

On Leap 15.1 it looks like follows. After `zypper in pcp` the following
directory permissions are set:

 # ls -lhd /var/lib/pcp/tmp
 drwxrwxr-x  5 pcp  pcp  4.0K 19. Mai 15:08 /var/lib/pcp/tmp

After calling chkstat the following happens.

 # chkstat --system
 Checking permissions and ownerships - using the permissions files
        /etc/permissions
        /etc/permissions.easy
        /etc/permissions.d/postfix
        /etc/permissions.d/texlive
        /etc/permissions.d/texlive.texlive
        /etc/permissions.local
 setting /var/lib/pcp/tmp/ to root:root 1777. (wrong owner/group pcp:pcp
permissions 0775)
 setting /var/lib/pcp/tmp/pmlogger/ to root:root 1777. (wrong owner/group pcp:pcp
permissions 0775)
```

setting /var/lib/pcp/tmp/pmie/ to root:root 1777. (wrong owner/group pcp:pcp permissions 0775)

```
# ls -lhd /var/lib/pcp/tmp
drwxrwxrwt 5 root root 4.0K 19. Mai 15:08 /var/lib/pcp/tmp
```

So the directories previously owned by pcp:pcp with mode 0775 are now public sticky bit directories again. Depending on how the directories are used by the pcp programs this can lead to security issues. In any case it is a terrible inconsistency and unexpected for the pcp package.

This happens only when the "easy" permissions profile is set. On SLE the "secure" permissions profile is the default. There the directories would end up as root:root with permissions 0755, thereby probably only breaking pcp.

On current Tumbleweed the situation regarding security is not that bad, because the `chkstat` tool has a number of security measures builtin that prevent lowering the security. There the output looks like follows:

```
# chkstat --system
/var/lib/pcp/tmp/: has unexpected owner. refusing to correct due to unknown integrity.
/var/lib/pcp/tmp/pmdabash/: on an insecure path - /var/lib/pcp/tmp has different non-root owner who could tamper with the file.
/var/lib/pcp/tmp/mmv/: on an insecure path - /var/lib/pcp/tmp has different non-root owner who could tamper with the file.
/var/lib/pcp/tmp/pmlogger/: on an insecure path - /var/lib/pcp/tmp has different non-root owner who could tamper with the file.
/var/lib/pcp/tmp/pmie/: on an insecure path - /var/lib/pcp/tmp has different non-root owner who could tamper with the file.
```

What needs to be done to fix this is to remove the entries from the permission package's profiles. Also in all codestreams where pcp is maintained.

Matthias Gerstner 2020-05-19 13:27:39 UTC Comment 2

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 2020-05-19 13:28:23 UTC Comment 3

Internal CRD: 2020-08-17 or earlier

David Disseldorp 2020-05-19 14:51:02 UTC Comment 4

(In reply to Matthias Gerstner from comment #1)
...

> What needs to be done to fix this is to remove the entries from the
> permission
> package's profiles. Also in all codestreams where pcp is maintained.

Hmm, I seem to recall that these profile entries were added around the time that some tempdir races were fixed. Since then there was some further work on privilege separation (e.g. splitting out /proc parsers etc. from main daemons) so that most services now run as pcp.

Matthias Gerstner 2020-05-28 09:58:12 UTC Comment 5

I will remove the permissions entries for pcp completely from Factory.

All maintained codestreams of pcp look to be also affected by this issue. So we will need backports to the permissions package in the respective codestreams.

A problem is that even when the permissions package is corrected, possibly wrong permissions will remain for the pcp directories. Thus we might need to ship "empty"/fake updates for pcp to get the permissions actually fixed via RPM.

I'll also have to look into the security situation if there are actual attack vectors introduced due to the wrong permissions.

David Disseldorp 2020-05-28 11:39:52 UTC Comment 6

(In reply to Matthias Gerstner from comment #5)

> I will remove the permissions entries for pcp completely from Factory.
>
> All maintained codestreams of pcp look to be also affected by this issue. So
> we will need backports to the permissions package in the respective
> codestreams.
>
> A problem is that even when the permissions package is corrected, possibly
> wrong permissions will remain for the pcp directories. Thus we might need to
> ship "empty"/fake updates for pcp to get the permissions actually fixed via
> RPM.

That sounds like a reasonable approach to me.

> I'll also have to look into the security situation if there are actual attack
> vectors introduced due to the wrong permissions.

Thanks.

Matthias Gerstner 2020-06-03 13:30:06 UTC Comment 7

I will start updates for the permissions package to remove the pcp entries.

It's a bit complex, since the permissions package has different maintained codestreams than the pcp package. It looks like the following permissions codestreams need to be addressed:

SUSE:SLE-12-SP4:Update
SUSE:SLE-12-SP5:Update
SUSE:SLE-15:GA
SUSE:SLE-15-SP1:GA
SUSE:SLE-15-SP2:GA

15-SP2:GA is still under development and should be done last, because it's publically visible in OBS and thus break the embargo.

Swamp Workflow Management 2020-07-06 19:13:21 UTC Comment 17

SUSE-SU-2020:1860-1: An update that contains security fixes can now be installed.

Category: security (moderate)
Bug References: 1171883
CVE References:
Sources used:
SUSE Linux Enterprise Module for Basesystem 15-SP1 (src): permissions-20181116-9.35.1

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 2020-07-06 19:19:31 UTC Comment 18

SUSE-SU-2020:1857-1: An update that contains security fixes can now be installed.

Category: security (moderate)
Bug References: 1171883
CVE References:
Sources used:
SUSE Linux Enterprise Server 12-SP4 (src): permissions-20170707-3.24.1

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 2020-07-06 19:20:13 UTC Comment 19

SUSE-SU-2020:1858-1: An update that contains security fixes can now be installed.

Category: security (moderate)
Bug References: 1171883
CVE References:
Sources used:
SUSE Linux Enterprise Server for SAP 15 (src): permissions-20180125-3.27.1
SUSE Linux Enterprise Server 15-LTSS (src): permissions-20180125-3.27.1
SUSE Linux Enterprise High Performance Computing 15-LTSS (src): permissions-20180125-3.27.1
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src): permissions-20180125-3.27.1

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 2020-07-14 10:15:44 UTC Comment 20

openSUSE-SU-2020:0957-1: An update that contains security fixes can now be installed.

Category: security (moderate)
Bug References: 1171883
CVE References:
Sources used:
openSUSE Leap 15.1 (src): permissions-20181116-lp151.4.24.1

Matthias Gerstner 2020-07-14 11:10:43 UTC Comment 21

I looked into the pcp code base to find out whether this issue has security relevance. The 'secure' and 'paranoid' profile settings will only break pcp programs, because they can no longer place files in the expected locations. The 'easy' profile setting is more dangerous, however. Since these settings give the respective directories world-writeable sticky-bit permissions, anybody can place files in there.

pcp has got a huge code base so I won't completely review everything. The base directory /var/lib/pcp/tmp is configured via the PCP_TMP_DIR setting in /etc/pcp.conf. Within the code this setting is queried via `pmGetConfig("PCP_TMP_DIR")`. This setting is used at least in libpcp, pmdas, mpieconf, mpie and pmlogger. Each individual utility uses one of the sub-directories like /var/lib/pcp/tmp/pmie.

Some of the files are memory-mapped by the tools. Some files contain binary data structures. The pmie sub-directory seems to contain binary data for each process in the system. This means an attacker could place fake data there, or data that causes the pcp programs to crash or otherwise misbehave. Since the pcp daemons seems to run under the unprivileged pcp user a local root exploit will not be that easy, at least.

I suggest we assign a single CVE for this, because otherwise we'd need to pull a dozen or even more of them and would need to analyze this situation in detail and that's not really efficient.

Johannes Segitz 2020-07-14 11:19:30 UTC Comment 22

Please use CVE-2020-8025 to track this

Matthias Gerstner 2021-01-21 09:52:46 UTC Comment 23

Somehow we failed to keep the permissions SUSE:SLE-15-SP2:Update codestream in sync with our GitHub SLE-15-SP2 branch. This the fix in that codestream has been missing up until now.

I just submitted a maintenance update for it.

Since we are dropping permissions from the profiles, future `chkstat --system` invocations will *not* fix possibly wrong permissions. The pcp package needs to reapply its regular permissions for these paths. So we might need to create

pseudo updates for pcp after the permissions are finally fixed in all codestreams.

Marcus Meissner 2021-01-22 10:47:38 UTC Comment 25

I think the only safe way, and what we used previously, is keep the permissions of the binaries, but set them the their regular RPM permissions e.g. 0755 .

Matthias Gerstner 2021-01-22 11:02:13 UTC Comment 26

(In reply to meissner@suse.com from comment #25)

> I think the only safe way, and what we used previously, is keep the
> permissions of the binaries, but set them the their regular RPM permissions
> e.g. 0755 .

That would mean we would need to do another update round. And there is no defined end to when these "safety" entries can be dropped. We just got rid of some of these kind of fixup entries that lingered in the permissions package for more than a decade.

It also brings the problem that again the actual package's permissions and what the permissions package sets can diverge. It's a big mess :-(

Swamp Workflow Management 2021-01-22 17:25:50 UTC Comment 27

SUSE-SU-2021:0197-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1171883
CVE References: CVE-2020-8025
JIRA References:
Sources used:
SUSE Linux Enterprise Module for Basesystem 15-SP2 (src): permissions-20181224-23.3.1

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.

Matthias Gerstner 2021-03-10 13:21:59 UTC Comment 28

Reassigning to pcp maintainer. Can you please submit "empty" updates for pcp in codestreams SUSE:SLE-12:Update and SUSE:SLE-15:Update such that the permissions of /var/lib/pcp/tmp/pmlogger & friends are corrected with the update?

In SLE-15-SP1 there already is an update available that fixes this.

Swamp Workflow Management 2021-04-21 16:25:52 UTC Comment 29

SUSE-SU-2021:1292-1: An update that contains security fixes can now be installed.

Category: security (moderate)
Bug References: 1123311,1171883,1181571
CVE References:
JIRA References:
Sources used:
SUSE Linux Enterprise Server for SAP 15 (src): pcp-3.11.9-5.11.5
SUSE Linux Enterprise Server 15-LTSS (src): pcp-3.11.9-5.11.5
SUSE Linux Enterprise High Performance Computing 15-LTSS (src): pcp-3.11.9-5.11.5
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src): pcp-3.11.9-5.11.5

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 2021-07-09 19:23:57 UTC Comment 30

SUSE-SU-2021:2280-1: An update that solves three vulnerabilities and has 11 fixes is now available.

Category: security (moderate)
Bug References:
1047247,1050467,1093414,1097665,1123886,1150734,1155939,1157198,1160594,1160764,11617
CVE References: CVE-2019-3688,CVE-2019-3690,CVE-2020-8013
JIRA References:
Sources used:
SUSE Linux Enterprise Server 12-SP5 (src): permissions-20170707-6.4.1

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.

Petr Gajdos 2022-04-25 12:40:25 UTC Comment 36

Easiest submit request I had ever made. Hopefully it is what you wanted, welcome to correct me.

Submitted for 12,15/pcp.

I believe all fixed.

Swamp Workflow Management 2022-05-03 19:24:53 UTC Comment 38

SUSE-SU-2022:1509-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1171883
CVE References: CVE-2020-8025
JIRA References:
Sources used:

```
openSUSE Leap 15.4 (src):    pcp-3.11.9-150000.5.14.1
openSUSE Leap 15.3 (src):    pcp-3.11.9-150000.5.14.1

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 2022-05-27 19:16:08 UTC Comment 39

```
SUSE-SU-2022:1873-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1171883
CVE References: CVE-2020-8025
JIRA References:
Sources used:
SUSE Linux Enterprise Software Development Kit 12-SP5 (src):    pcp-3.11.9-6.17.1

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.
```