~~Bug 1180685 - (CVE-2021-23240) VUL-0: CVE-2021-23240: sudo: Possible Symlink Attack in SELinux Context in `sudoedit`~~

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: [none]
Whiteboard: CVSSv3.1:SUSE:CVE-2021-23240:7.8:(AV:...
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2021-01-08 09:34 UTC by Matthias Gerstner
Modified: 2021-10-14 09:38 UTC (History)
CC List: 5 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 2021-01-08 09:34:22 UTC — Description

```
Tracking for issue d) from ~~bug 1171720~~. This is still under embargo but will
be published somewhen next week in sudo 1.9.5.

  If SELinux is enabled on a system then `sudoedit` uses alternate code
  paths to create temporary files and to copy temporary files to target
  files, namely `selinux_edit_copy_tfiles()` and
  `selinux_edit_create_tfiles()`. Both functions employ `chown()` system
  calls which follow symlinks.

  Especially in `selinux_edit_copy_tfiles()` a `chown()` to the target
  user is performed on a temporary file path that is owned by the
  unprivileged user in e.g. /var/tmp. The unprivileged user could remove
  this file and replace it by a symlink to a another file, that would be
  followed by `sudoedit` to change its ownership.

  When SELinux is in enforce mode then it should prevent such a thing to
  happen. But a system might run in SELinux permissive mode in which case
  the SELinux logic in `sudoedit` would still trigger but the protection
  effect would be gone.
```

Matthias Gerstner 2021-01-08 10:11:09 UTC — Comment 1

```
Regarding affectedness Factory, SLE-15 and SLE-12 based codestreams are
equally affected. SLE-11 based codestreams don't contain SELinux support yet
so they aren't affected with this particular issue.
```

Matthias Gerstner 2021-01-11 13:23:30 UTC — Comment 2

```
Upstream has published the bugfixes now. The fixing commit is
12800:8fcb36ef422a. Please provide submissions for affected codestreams.
```

Simon Lees 2021-01-25 04:25:04 UTC — Comment 4

```
(In reply to Matthias Gerstner from comment #1)
> Regarding affectedness Factory, SLE-15 and SLE-12 based codestreams are
> equally affected. SLE-11 based codestreams don't contain SELinux support yet
> so they aren't affected with this particular issue.


SLE-12-SP2 doesn't contain sudo_edit_mktemp or selinux_edit_create_tfiles yet, so
i'm not 100% certain if they are affected by this issue. If they are they will
require a completely different fix and it will miss the current update round.
```

Matthias Gerstner 2021-01-25 09:53:12 UTC — Comment 5

```
(In reply to simonf.lees@suse.com from comment #4)
> SLE-12-SP2 doesn't contain sudo_edit_mktemp or selinux_edit_create_tfiles
> yet, so i'm not 100% certain if they are affected by this issue. If they are
> they will require a completely different fix and it will miss the current
> update round.

It doesn't look like there is any SELinux specific sudoedit code yet in this
codestream. Also no trace of the plain `chown()` call. So I would consider
this codestream as not affected.
```

Swamp Workflow Management 2021-01-26 23:16:20 UTC Comment 6

```
SUSE-SU-2021:0226-1: An update that solves three vulnerabilities and has one errata
is now available.

Category: security (important)
Bug References: 1180684,1180685,1180687,1181090
CVE References: CVE-2021-23239,CVE-2021-23240,CVE-2021-3156
JIRA References:
Sources used:
SUSE OpenStack Cloud Crowbar 9 (src):    sudo-1.8.20p2-3.20.1
SUSE OpenStack Cloud Crowbar 8 (src):    sudo-1.8.20p2-3.20.1
SUSE OpenStack Cloud 9 (src):    sudo-1.8.20p2-3.20.1
SUSE OpenStack Cloud 8 (src):    sudo-1.8.20p2-3.20.1
SUSE Linux Enterprise Server for SAP 12-SP4 (src):    sudo-1.8.20p2-3.20.1
SUSE Linux Enterprise Server for SAP 12-SP3 (src):    sudo-1.8.20p2-3.20.1
SUSE Linux Enterprise Server 12-SP4-LTSS (src):    sudo-1.8.20p2-3.20.1
SUSE Linux Enterprise Server 12-SP3-LTSS (src):    sudo-1.8.20p2-3.20.1
SUSE Linux Enterprise Server 12-SP3-BCL (src):    sudo-1.8.20p2-3.20.1
SUSE Enterprise Storage 5 (src):    sudo-1.8.20p2-3.20.1
HPE Helion Openstack 8 (src):    sudo-1.8.20p2-3.20.1

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 2021-01-26 23:17:52 UTC Comment 7

```
SUSE-SU-2021:0227-1: An update that solves three vulnerabilities and has one errata
is now available.

Category: security (important)
Bug References: 1180684,1180685,1180687,1181090
CVE References: CVE-2021-23239,CVE-2021-23240,CVE-2021-3156
JIRA References:
Sources used:
SUSE Manager Server 4.0 (src):    sudo-1.8.22-4.15.1
SUSE Manager Retail Branch Server 4.0 (src):    sudo-1.8.22-4.15.1
SUSE Manager Proxy 4.0 (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Server for SAP 15-SP1 (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Server for SAP 15 (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Server 15-SP1-LTSS (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Server 15-SP1-BCL (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Server 15-LTSS (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Module for Basesystem 15-SP3 (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Module for Basesystem 15-SP2 (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise Module for Basesystem 15-SP1 (src):    sudo-1.8.22-4.15.1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS (src):    sudo-1.8.22-
4.15.1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS (src):    sudo-
1.8.22-4.15.1
SUSE Linux Enterprise High Performance Computing 15-LTSS (src):    sudo-1.8.22-
4.15.1
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src):    sudo-1.8.22-
4.15.1
SUSE Enterprise Storage 6 (src):    sudo-1.8.22-4.15.1
SUSE CaaS Platform 4.0 (src):    sudo-1.8.22-4.15.1

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 2021-01-26 23:19:11 UTC Comment 8

```
SUSE-SU-2021:0225-1: An update that solves three vulnerabilities and has one errata
is now available.

Category: security (important)
Bug References: 1180684,1180685,1180687,1181090
CVE References: CVE-2021-23239,CVE-2021-23240,CVE-2021-3156
JIRA References:
Sources used:
SUSE Linux Enterprise Software Development Kit 12-SP5 (src):    sudo-1.8.27-4.6.1
SUSE Linux Enterprise Server 12-SP5 (src):    sudo-1.8.27-4.6.1

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 2021-01-27 11:15:50 UTC Comment 9

```
openSUSE-SU-2021:0170-1: An update that solves three vulnerabilities and has one
errata is now available.

Category: security (important)
Bug References: 1180684,1180685,1180687,1181090
CVE References: CVE-2021-23239,CVE-2021-23240,CVE-2021-3156
JIRA References:
Sources used:
openSUSE Leap 15.2 (src):    sudo-1.8.22-lp152.8.6.1
```

Swamp Workflow Management 2021-01-27 11:17:07 UTC Comment 10

```
openSUSE-SU-2021:0169-1: An update that solves three vulnerabilities and has one
errata is now available.

Category: security (important)
Bug References: 1180684,1180685,1180687,1181090
CVE References: CVE-2021-23239,CVE-2021-23240,CVE-2021-3156
JIRA References:
Sources used:
openSUSE Leap 15.1 (src):    sudo-1.8.22-lp151.5.12.1
```

Simon Lees 2021-05-11 01:07:59 UTC Comment 12

```
Should be done reassigning to security
```

Robert Frohl 2021-10-14 09:38:23 UTC Comment 16

```
done
```