~~Bug 1180684 - (CVE-2021-23239) VUL-0: CVE-2021-23239: sudo: Possible Dir Existence Test due to Race Condition 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-2021-23239:2.5:(AV:...
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2021-01-08 09:27 UTC by Matthias Gerstner
Modified: 2021-10-14 07:28 UTC (History)
CC List: 7 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 09:27:14 UTC Description

```
Tracking for item c) in ~~bug 1171788~~. This is still embargoed but will be
published somewhen next week with sudo 1.9.5.

  # c) Possible Dir Existence Test due to Race Condition in `sudoedit`

  The `sudoedit` personality by default wants to prevent that the edited
  file is in any way under control of an unprivileged user. This logic is
  rooted in `sudo_edit_open()` / `sudo_edit_open_nonwritable()`. It
  follows the complete file path from the file system root downwards and
  avoids symlinks in directories that are writable by unprivileged users.

  There is a corner case, however, when the target file does not exist
  yet. This is handled in `sudo_edit.c:545`. `errno` will be set to
  `ENOENT`, because the file didn't exist yet. Now the code checks the
  parent directory of the path for existence and whether it is a
  directory. If this is both true then the edit operation continues in the
  expectation that later on a new file will be created. The check is done
  using `stat()`, however, thus if the parent directory is under control
  of the unprivileged user, it can try to win a race condition and place
  an arbitrary symlink at the parent directory location just in time for
  the check in `sudo_edit.c:549` to succeed.

  This means the precondition covered in `sudo_edit.c:576` is no longer
  true ("editing files in a writable directory is not permitted"). As far
  as I can see this only allows an attacker to test for existence of
  directories in arbitrary locations, if the target user is root, because
  `sudoedit` behaves differently if the link target exists and is a
  directory, or if it doesn't exist or isn't a directory. It *cannot* be
  used to write to arbitrary locations, because the write operation
  happens in `sudo_edit.c:1043` via `sudo_edit_copy_tfiles()`, which uses
  `sudo_edit_open()`, this time with `O_CREAT` to open the target file.
  This will not follow a symlink this time.

  Example: A regular user 'testuser' is for some reason allowed to edit
  the file /home/testuser/subdir/file with root privileges and without
  password entry.

  ```
  sudoedit ~/subdir/file
  ```

  Initially ~/subdir is empty or doesn't exist. The logic in
  `sudo_edit.c:545` will come into play. 'testuser' wins the race to
  create a symlink:

  ```
  ln -s /root/.gnupg ~/subdir
  ```

  If /root/.gnupg exists then `sudoedit` will now open the editor, if it
  doesn't exist it will fail with

  ```
  sudoedit: /home/testuser/subdir/file: No such file or directory
  ```
```

Matthias Gerstner 2021-01-08 10:04:50 UTC Comment 1

```
I have looked into the maintained codestreams. Factory, SLE-15 and SLE-12
based codestreams are all equally affected and have similar code in this spot.

SLE-11 based code already has sudoedit functionality, but the whole logic to
check the parent directories of the target path is not existing yet. This
means SLE-11 based codestreams could have a bunch of issues in this area if
```

the target path is somehow under control of the invoking user. This would be difficult to fix there.

Matthias Gerstner 2021-01-11 13:21:11 UTC Comment 2

The bugfixes have been published now by upstream. The fixing commit is 12799:ea19d0073c02. Please provide submissions for affected codestreams.

Swamp Workflow Management 2021-01-26 23:16:14 UTC Comment 5

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 23:17:45 UTC Comment 6

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 23:19:04 UTC Comment 7

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 11:15:42 UTC Comment 8

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 11:17:00 UTC Comment 9

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

Swamp Workflow Management 2021-01-27 14:20:52 UTC Comment 10

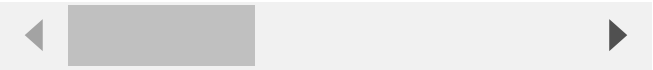
```
SUSE-SU-2021:0232-1: An update that fixes two vulnerabilities is now available.

Category: security (important)
Bug References: 1180684,1181090
CVE References: CVE-2021-23239,CVE-2021-3156
JIRA References:
Sources used:
SUSE OpenStack Cloud 7 (src):    sudo-1.8.10p3-10.29.1
SUSE Linux Enterprise Server for SAP 12-SP2 (src):    sudo-1.8.10p3-10.29.1
SUSE Linux Enterprise Server 12-SP2-LTSS (src):    sudo-1.8.10p3-10.29.1
SUSE Linux Enterprise Server 12-SP2-BCL (src):    sudo-1.8.10p3-10.29.1

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.
```

Marcus Meissner 2021-01-28 08:31:32 UTC Comment 11

```
would SLE11 sudo versions also be affected?
```

Matthias Gerstner 2021-02-02 09:31:53 UTC Comment 14

```
(In reply to yuliu@suse.com from comment #13)
> Please confirm whether sudo-1.8.10p3-10.29.1.x86_64 is successfully repaired. The
```



```
You may have posted in the wrong bug. Where does this reproducer come from?
```

Simon Lees 2021-05-11 01:08:22 UTC Comment 18

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

Marcus Meissner 2021-05-12 11:27:57 UTC Comment 19

```
done
```
