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

~~Bug 1182777 - (CVE-2021-25316) VUL-0: CVE-2021-25316: s390-tools: Local DoS of VM live migration due to use of static tmp files in detach_disks.sh~~

Status: RESOLVED FIXED

Classification: Novell Products
Product: SUSE Security Incidents
Component: Incidents
Version: unspecified
Hardware: S/390-64 Other

Priority: P4 - Low **Severity**: Normal
Target Milestone: ---
Assigned To: Security Team bot
QA Contact: Security Team bot

URL: https://smash.suse.de/issue/278588/
Whiteboard: CVSSv3.1:SUSE:CVE-2021-25316:6.1:(AV:...
Keywords:

Depends on:
Blocks: ~~1180877~~
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2021-02-25 18:03 UTC by Wolfgang Frisch
Modified: 2021-04-19 16:33 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.

Wolfgang Frisch 2021-02-25 18:03:40 UTC Description

+++ This bug was initially created as a clone of ~~Bug #1180877~~ +++

~~~~
In openSUSE:Factory/s390-tools/detach_disks.sh, predictable /tmp files are used.

```
COOKIE=$(mcookie)
DASDFILE=/tmp/dasd.list.${COOKIE}
DETFILE=/tmp/detach.disks.${COOKIE}
KEEPFILE=/tmp/keep.disks.${COOKIE}
NICFILE=/tmp/nic.list.${COOKIE}
FAILFILE=/tmp/error.${COOKIE}
```

The cookie is an unpredictable 32 character hash. However, since the script does
not create all temp files at once, we can watch /tmp with inotify, get the cookie
from the first created file, and predict the remaining paths.

Example run of detach_disks.sh, logged with `inotifywait -m -e create /tmp/`:
```
/tmp/ CREATE dasd.list.ce4955d2133c9c6e425791e39af56340
/tmp/ CREATE detach.disks.ce4955d2133c9c6e425791e39af56340
/tmp/ CREATE keep.disks.ce4955d2133c9c6e425791e39af56340
/tmp/ CREATE nic.list.ce4955d2133c9c6e425791e39af56340
```

Steps to reproduce:
As root:
- configure ZVM_DISKS_TO_DETACH in /etc/sysconfig/virtsetup
  e.g. ZVM_DISKS_TO_DETACH="1"
- mkdir /test
- touch /test/shadow

As an unprivileged user:
- Run the attached `PoC-detach_disks.py`

As root:
- /usr/lib/systemd/scripts/detach_disks.sh

Consequences:
- If fs.protected_symlinks = 1 (default on SLE),
  the unprivileged user can deny the service of detach_disks.sh.
- If fs.protected_symlinks = 0,
  the unprivileged user can overwrite arbitrary files.
~~~~

Wolfgang Frisch 2021-02-25 18:04:19 UTC Comment 1

```
Created attachment 846546 [details]
PoC-detach_disks.py
```

Wolfgang Frisch 2021-02-25 18:10:59 UTC Comment 2

```
One solution would be to confine all the temp files in a securely created temporary
directory, e.g. with tmpdir=$(mktemp -d /tmp/detach_disks.XXXXXX).
```

Mark Post 2021-02-26 20:37:23 UTC Comment 4

```
I am considering making the following change. It should eliminate any possibility
of "guessing" the filenames that are being created. Let me know what you think.
--- detach_disks.sh.20160524    2016-05-24 15:14:19.000000000 -0400
+++ detach_disks.sh     2021-02-26 10:36:50.946676687 -0500
```

```
@@ -1,11 +1,10 @@
 #!/bin/sh

-COOKIE=$(mcookie)
-DASDFILE=/tmp/dasd.list.${COOKIE}
-DETFILE=/tmp/detach.disks.${COOKIE}
-KEEPFILE=/tmp/keep.disks.${COOKIE}
-NICFILE=/tmp/nic.list.${COOKIE}
-FAILFILE=/tmp/error.${COOKIE}
+DASDFILE=/tmp/dasd.list.${mcookie}
+DETFILE=/tmp/detach.disks.${mcookie}
+KEEPFILE=/tmp/keep.disks.${mcookie}
+NICFILE=/tmp/nic.list.${mcookie}
+FAILFILE=/tmp/error.${mcookie}

 function expand_RANGE(){
 local RANGE=${1}
```

Wolfgang Frisch 2021-02-28 21:32:30 UTC Comment 6

```
(In reply to Mark Post from comment #4)
> I am considering making the following change. It should eliminate any
> possibility of "guessing" the filenames that are being created. Let me know
> what you think.
> --- detach_disks.sh.20160524  2016-05-24 15:14:19.000000000 -0400
> +++ detach_disks.sh   2021-02-26 10:36:50.946676687 -0500
> @@ -1,11 +1,10 @@
>  #!/bin/sh
>
> -COOKIE=$(mcookie)
> -DASDFILE=/tmp/dasd.list.${COOKIE}
> -DETFILE=/tmp/detach.disks.${COOKIE}
> -KEEPFILE=/tmp/keep.disks.${COOKIE}
> -NICFILE=/tmp/nic.list.${COOKIE}
> -FAILFILE=/tmp/error.${COOKIE}
> +DASDFILE=/tmp/dasd.list.${mcookie}
> +DETFILE=/tmp/detach.disks.${mcookie}
> +KEEPFILE=/tmp/keep.disks.${mcookie}
> +NICFILE=/tmp/nic.list.${mcookie}
> +FAILFILE=/tmp/error.${mcookie}
>
>  function expand_RANGE(){
>  local RANGE=${1}


Thanks for the quick reaction.

This is OK in principal but there's a typo in the suggested changes: It should be
$(mcookie) instead of ${mcookie}, which refers to a non-existent variable.

The standard `mktemp` utility would be an acceptable alternative, e.g.:
DASDFILE=$(/tmp/dasd.list.XXXXXX)
```

Wolfgang Frisch 2021-02-28 21:33:13 UTC Comment 7

```
DASDFILE=$(mktemp /tmp/dasd.list.XXXXXX)
```

Mark Post 2021-02-28 23:22:39 UTC Comment 8

```
(In reply to Wolfgang Frisch from comment #6)
-snip-
> This is OK in principal but there's a typo in the suggested changes: It
> should be $(mcookie) instead of ${mcookie}, which refers to a non-existent
> variable.


Argh. You're right, of course.
```

OBSbugzilla Bot 2021-03-01 00:10:06 UTC Comment 9

```
This is an autogenerated message for OBS integration:
This bug (1182777) was mentioned in
https://build.opensuse.org/request/show/875842 Factory / s390-tools
```

Johannes Segitz 2021-03-01 09:24:10 UTC Comment 11

```
Please use CVE-2021-25316 for this
```

OBSbugzilla Bot 2021-03-01 16:50:07 UTC Comment 13

```
This is an autogenerated message for OBS integration:
This bug (1182777) was mentioned in
https://build.opensuse.org/request/show/876032 Factory / s390-tools
```

OBSbugzilla Bot 2021-03-08 23:20:07 UTC Comment 16

```
This is an autogenerated message for OBS integration:
This bug (1182777) was mentioned in
https://build.opensuse.org/request/show/877835 Factory / s390-tools
```

Mark Post 2021-03-09 21:19:32 UTC Comment 18

```
Could you remove 1180877 from the "Depends on" for this bug? I can't mark it
resolved with that there, and I can't remove it, either. Thanks.
```

Johannes Segitz 2021-03-10 06:53:09 UTC Comment 19

```
Done. Leaving the needinfo for Wolfgang.

@Wolfgang: If you clone the bug bugzilla creates (for us) nonsensical
relationships. You need to adjust it so that the new bug blocks the parent bug so
that the closed bugs can be closed before we close the tracker bug
```

Mark Post 2021-03-10 17:16:30 UTC Comment 20

Updated packages have been submitted to openSUSE:Factory, SLE-12-SP5, and SLE-15-SP2.

Mark Post 2021-03-10 17:19:08 UTC Comment 21

Updated package has been submitted to SLE-15-SP3 as well.

Alexandros Toptsoglou 2021-03-11 10:07:45 UTC Comment 22

(In reply to Mark Post from comment #21)

> Updated package has been submitted to SLE-15-SP3 as well.

Please do not resolve security bugs, instead assign back to security team when you are done for a final review.

Swamp Workflow Management 2021-03-12 20:17:31 UTC Comment 23

```
SUSE-SU-2021:0776-1: An update that solves one vulnerability and has two fixes is
now available.

Category: security (important)
Bug References: 1182777,1182876,1183041
CVE References: CVE-2021-25316
JIRA References:
Sources used:
SUSE Linux Enterprise Server 12-SP5 (src):    s390-tools-2.1.0-18.29.1

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.
```

Swamp Workflow Management 2021-03-12 20:25:18 UTC Comment 24

```
SUSE-SU-2021:0777-1: An update that solves one vulnerability and has three fixes is
now available.

Category: security (important)
Bug References: 1176574,1182777,1182876,1183040
CVE References: CVE-2021-25316
JIRA References:
Sources used:
SUSE Linux Enterprise Module for Basesystem 15-SP2 (src):    s390-tools-2.11.0-
9.20.1

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.
```

Wolfgang Frisch 2021-04-19 16:33:51 UTC Comment 25

Released!

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

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