~~Bug 1169385~~ - (CVE-2020-8019) VUL-0: CVE-2020-8019: syslog-ng: Local privilege escalation from new to root in %post

Status:	RESOLVED FIXED		

- Create test case
- Clone This Bug

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:	https://smash.suse.de/issue/257020/
Whiteboard:	
Keywords:	
Depends on:	
Blocks:	
	Show dependency tree / graph

Reported:	2020-04-14 08:13 UTC by Johannes Segitz
Modified:	2020-06-29 09:38 UTC (History)
CC List:	6 users (show)
See Also:	
Found By:	---
Services Priority:	
Business Priority:	
Blocker:	---

Attachments

diff of syslog-ng.spec (1.39 KB, text/plain)   Details
2020-04-15 08:55 UTC, Thomas Blume

Add an attachment (proposed patch, testcase, etc.)   View All

---

┌─Note──┐
│ You need to log in before you can comment on or make changes to this bug. │
└──┘

Johannes Segitz   2020-04-14 08:13:05 UTC   Description

```
POC:

sh-4.4$ id
uid=453(news) gid=450(news) groups=450(news)
context=unconfined_u:unconfined_r:unconfined_t:s0
sh-4.4$ cd /var/log/news/
sh-4.4$ rm news.err
sh-4.4$ ln -s /etc/shadow news.err

As root force reinstall of syslog-ng
zypper in -f syslog-ng

After that:
sh-4.4$ ls -lah /etc/shadow
-rw-r-----. 1 news news 1.2K Apr 14 10:03 /etc/shadow


The issue is this section in %post
364 mkdir -p -m 0750 var/log/news
365 chown news:news  var/log/news
366 touch var/log/news/news.crit;    chmod 640 var/log/news/news.crit
367 chown news:news var/log/news/news.crit
368 touch var/log/news/news.err;     chmod 640 var/log/news/news.err
369 chown news:news var/log/news/news.err
370 touch var/log/news/news.notice; chmod 640 var/log/news/news.notice
371 chown news:news var/log/news/news.notice

As /var/log/news is owned by news it's dangerous to operate as root in this
directory. SLE 12 and Factory are affected. I would just remove this construct and
let rpm create the files
```

Johannes Segitz   2020-04-14 08:16:07 UTC   Comment 1

```
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
- do not submit this into OBS (e.g. fix Leap) until this is public

In accordance with our policy we will make this issue public latest at
Internal CRD: 2020-07-13 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.

This is an internal finding, so we can make it public at any time we chose, but
please coordinate with us.

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

Thomas Blume   2020-04-14 08:36:48 UTC   Comment 2

```
Hm, AFAIK, syslog-ng is not shipped anymore with the currently supported SLES
version.
According to https://www.suse.com/releasenotes/x86_64/SUSE-SLES/12/ it is part of
the Legacy Module for which support seems to have expired too.
```

So, I'm not sure for which codestreams I will have to provide the fix.

Anyone who knows?

Johannes Segitz   2020-04-14 09:21:45 UTC   Comment 3

(In reply to Thomas Blume from comment #2)
According to is_maintained:

```
SLE-DEBUGINFO_11-SP1-TERADATA          SUSE:SLE-11-SP1:Update
SLE-SERVER_11-SP1-TERADATA             SUSE:SLE-11-SP1:Update
SLE-DEBUGINFO_11-SP3-TERADATA          SUSE:SLE-11-SP1:Update
SLE-SERVER_11-SP3-TERADATA             SUSE:SLE-11-SP1:Update
SLE-Module-Legacy_12                   SUSE:SLE-12:Update
SLE-SAP_12-SP1                         SUSE:SLE-12:Update
```

So SLE-11-SP1 and SLE-12 please. CCing peter@czanik.hu for openSUSE

---

peter czanik   2020-04-15 07:26:48 UTC   Comment 4

Could you share the proposed fix for SLES? I'll test it on openSUSE on a local
build.

Note: current Base:System:syslog-ng is not yet accepted to Factory. Someone
submitted an update to the latest version and some cleanup, which I accepted there,
but it needs some changes before it can go to Factory. As I see a June date for CVE
publication, I fix it independent of this. So, once this bug is public, we can go
the regular Base:System:syslog-ng -> Factory easily.

Thomas Blume   2020-04-15 08:55:34 UTC   Comment 5

Created attachment 835793 [details]
diff of syslog-ng.spec

Here is a diff of the specfile.
Johannes, does that match your proposal?

Johannes Segitz   2020-04-15 11:37:25 UTC   Comment 6

looks good, thanks

---

ming li   2020-04-21 07:34:37 UTC   Comment 9

I'm testing the update. I found a problem. When I upgrade the program to a new
version(3.6.4-12.6.1), the contents of the files in the previous news directory
will be cleared, and this problem will also be triggered during the forced or
upgraded installation of the same version of software. The tested old version of
the package does not have these problems(3.6.4-12.3.1), and the log will be kept
intact.

```
reproducer:
s12sp3:~ # rpm -qa|grep syslog-ng
syslog-ng-3.6.4-12.3.1.x86_64

s12sp3:~ # su news

news@s12sp3:/root> cd /var/log/news

news@s12sp3:/var/log/news> echo "abcdefghijk" > news.err

news@s12sp3:/var/log/news> cat news.err
abcdefghijk

news@s12sp3:/var/log/news> ll
total 4
-rw-r----- 1 news news  0 Apr 21 15:23 news.crit
-rw-r----- 1 news news 12 Apr 21 15:23 news.err
-rw-r----- 1 news news  0 Apr 21 15:23 news.notice

s12sp3:~ # zypper ar -f
http://download.suse.de/ibs/SUSE:/Maintenance:/14729/SUSE_Updates_SLE-Module-
Legacy_12_x86_64/ test

s12sp3:~ # zypper up syslog-ng

s12sp3:~ # rpm -qa|grep syslog-ng
syslog-ng-3.6.4-12.6.1.x86_64

s12sp3:~ # cat /var/log/news/news.err

s12sp3:~ # ll /var/log/news/
total 0
-rw-r----- 1 news news 0 Apr 16 15:44 news.crit
-rw-r----- 1 news news 0 Apr 16 15:44 news.err
-rw-r----- 1 news news 0 Apr 16 15:44 news.notice
```

The contents of the files will also be emptied during the forced or upgraded
installation of the same version of software:

```
s12sp3:~ # zypper ar -f
http://download.suse.de/ibs/SUSE:/Maintenance:/14729/SUSE_Updates_SLE-Module-
Legacy_12_x86_64/ test

s12sp3:~ # zypper in -f syslog-ng

s12sp3:~ # rpm -qa|grep syslog-ng
syslog-ng-3.6.4-12.6.1.x86_64

s12sp3:~ # su news

news@s12sp3:/root> cd /var/log/news

news@s12sp3:/var/log/news> echo "abcdefghijk" > news.err

news@s12sp3:/var/log/news> cat news.err
abcdefghijk

news@s12sp3:/var/log/news> ll
total 4
-rw-r----- 1 news news  0 Apr 16 15:44 news.crit
-rw-r----- 1 news news 12 Apr 21 15:04 news.err
-rw-r----- 1 news news  0 Apr 16 15:44 news.notice

s12sp3:~ # zypper in -f syslog-ng
```

```
Loading repository data...
Reading installed packages...
Forcing installation of 'syslog-ng-3.6.4-12.6.1.x86_64' from repository 'test'.
Resolving package dependencies...

The following package is going to be reinstalled:
  syslog-ng

1 package to reinstall.
Overall download size: 475.9 KiB. Already cached: 0 B. No additional space will be
used or freed after the operation.
Continue? [y/n/...? shows all options] (y):
Retrieving package syslog-ng-3.6.4-12.6.1.x86_64
(1/1), 475.9 KiB (  1.8 MiB unpacked)
Retrieving: syslog-ng-3.6.4-12.6.1.x86_64.rpm
.......................................................................
[done (207.4 KiB/s)]

Checking for file conflicts:
.......................................................................
[done]
(1/1) Installing: syslog-ng-3.6.4-12.6.1.x86_64
.......................................................................
[done]
Additional rpm output:
Updating /etc/sysconfig/syslog...

s12sp3:~ # ll /var/log/news
total 0
-rw-r----- 1 news news 0 Apr 16 15:44 news.crit
-rw-r----- 1 news news 0 Apr 16 15:44 news.err
-rw-r----- 1 news news 0 Apr 16 15:44 news.notice

s12sp3:~ # cat /var/log/news/news.err
```

```
this means it destroys the /var/log/news content during update, which is not so
good.

perhaps using something like %ghost files might help.
```

---

ming li   2020-04-21 08:06:59 UTC

```
It also removes the entire news directory during the downgrade:

reproducer:
s12sp3:~ # rpm -qa|grep syslog-ng
syslog-ng-3.6.4-12.6.1.x86_64

s12sp3:~ # su news

news@s12sp3:/root> cd /var/log/news/

news@s12sp3:/var/log/news> echo "abcdefghijk" > news.err

news@s12sp3:/var/log/news>  cat news.err
abcdefghijk

news@s12sp3:/var/log/news> ll
total 4
-rw-r----- 1 news news  0 Apr 16 15:44 news.crit
-rw-r----- 1 news news 12 Apr 21 15:51 news.err
-rw-r----- 1 news news  0 Apr 16 15:44 news.notice

s12sp3:~ # zypper in -f --oldpackage syslog-ng-3.6.4-12.3.1

s12sp3:~ # rpm -qa|grep syslog-ng
syslog-ng-3.6.4-12.3.1.x86_64

s12sp3:~ # ls /var/log/news
ls: cannot access '/var/log/news': No such file or directory

I think it's a regression.
```

Johannes Segitz   2020-04-21 08:39:33 UTC

```
I'm not sure if %ghost would work as that IIRC wouldn't create the file and set the
permissions as needed. Maybe marking it as %config could be abused, but that feels
pretty dirty
```

Thomas Blume   2020-04-21 11:06:58 UTC

```
(In reply to Johannes Segitz from comment #12)

> I'm not sure if %ghost would work as that IIRC wouldn't create the file and
> set the permissions as needed. Maybe marking it as %config could be abused,
> but that feels pretty dirty

So, the only chance I see is to move the old news directory away in a %pre script,
and cat the content of the old news files in the freshly created files in a %post
script.
Would that be ok?
```

Johannes Segitz   2020-04-21 13:45:57 UTC

```
(In reply to Thomas Blume from comment #13)
no that doesn't work as this would mean that root operates in a user controlled
directory. That is really hard to do right and almost impossible in bash.

Since %ghost doesn't work please give %config(noreplace) at try. Maybe someone with
more packaging knowledge has a better idea
```

---

peter czanik   2020-04-22 06:50:59 UTC

```
First of all a stupid question: is there still anything using these log files? I
did a quick search on Leap packages, so I might have overlooked something, but I
could not find anything news related.
```

```
Also, I did not have time yet for testing, so I might ask something stupid:

- how is it solved in rsyslog packaging?
- even if we remove news related stuff from %post, it remains a user owned
directory where the user still can delete files, create symlinks, etc. So, is this
really a solution?
- syslog-ng can create files and even directories on demand with proper user and
permissions, see: create-dirs(), dir-* at https://www.syslog-ng.com/technical-
documents/doc/syslog-ng-open-source-edition/3.16/administration-guide/31#TOPIC-
956501

Obviously #2 and #3 contradict each other, but with #3 news related directory and
file are only created if there is incoming log for news.

Another workaround idea: make the /var/log/news directory owned by root. That way
the news user can't do anything ugly and syslog-ng can still create log files owned
by news.

If all goes well, I can spend more time on it in the coming days.

CzP from syslog-ng upstream
```

Thomas Blume   2020-04-22 07:37:57 UTC   Comment 16

```
(In reply to peter czanik from comment #15)
> First of all a stupid question: is there still anything using these log
> files? I did a quick search on Leap packages, so I might have overlooked
> something, but I could not find anything news related.
>
> Also, I did not have time yet for testing, so I might ask something stupid:
>
> - how is it solved in rsyslog packaging?
> - even if we remove news related stuff from %post, it remains a user owned
> directory where the user still can delete files, create symlinks, etc. So,
> is this really a solution?
> - syslog-ng can create files and even directories on demand with proper user
> and permissions, see: create-dirs(), dir-* at
> https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-
> edition/3.16/administration-guide/31#TOPIC-956501
>
> Obviously #2 and #3 contradict each other, but with #3 news related
> directory and file are only created if there is incoming log for news.
>
> Another workaround idea: make the /var/log/news directory owned by root.
> That way the news user can't do anything ugly and syslog-ng can still create
> log files owned by news.

I guess for Leap another question would be, is syslog-ng still used by anyone? ;)

For SLES, I'm afraid we cannot go the way of syslog-ng autocreation of the news
files, since they were there in previous packages. syslog-ng in SLES is already far
into LTSS and changing the presence of files in a package at this stage of the
lifecycle is pretty problematic.
We have to be as less intrusive as possible for such legacy packages.
```

Johannes Segitz   2020-04-22 15:16:08 UTC   Comment 17

```
(In reply to peter czanik from comment #15)
> First of all a stupid question: is there still anything using these log files?
```
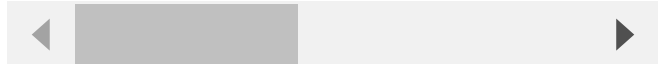


```
can't answer this, but usually there's at least one person using every oh so arcane
thing

> Also, I did not have time yet for testing, so I might ask something stupid:
>
> - how is it solved in rsyslog packaging?

rsyslog doesn't package any files in /var/log in openSUSE

> - even if we remove news related stuff from %post, it remains a user owned direct
```
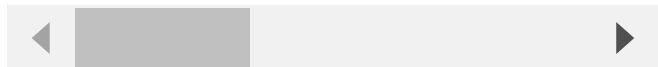


```
yes because that isn't the problem. The issue here it the ability to escalate your
privileges to root. Of course it would be better if the log files belonged to root,
but I assume that they need to belong to news so that this user can write into
these files

> - syslog-ng can create files and even directories on demand with proper user and
```



```
If we can configure syslog-ng to create the files when needed than this would be
the best solution if this is done in a secure way (either /var/log/news belonging
to root, see below, or syslog-ng being really careful when operating in a non-root
owned directory)

> Another workaround idea: make the /var/log/news directory owned by root. That way
```



```
That would work if syslog-ng is careful in how it does that. If you have a config
for that that I can test I can check if this is done in a secure way

> If all goes well, I can spend more time on it in the coming days.

Great to hear :)
```

peter czanik 2020-04-23 09:39:43 UTC

Comment 18

Yes, syslog-ng is still in use by SLES and Leap users. As all error messages direct
people to syslog-ng websites, most questions and bug reports land us upstream.
Many use my unofficial syslog-ng packages from OBS as well, both SLES and Leap.
Even on some less common architectures, like POWER and Aarch64 :)

If log files need to be created by the time of installation, then the only possible
workaround I see is to do some tests. Does something like this work from RPM?

if [[-L var/log/news/news.err]]; then echo "oops, var/log/news/news.err is a
symlink, skipping it"; else touch var/log/news/news.err; chmod 640
var/log/news/news.err ; fi

I'll post a syslog-ng configuration in the afternoon for creating news directory
and files on demand with proper rights. Practically it's adding the following
setting to all destinations within the news directory:

create-dirs(yes) dir-group("news") dir-owner("news") dir-perm(750)

I did not test it yet.

---

peter czanik 2020-04-23 10:26:09 UTC

Comment 19

Relevant part of the syslog-ng configuration for automagical directory creation:

```
"
#
# News-messages in separate files:
#
destination newscrit   { file("/var/log/news/news.crit"
    create-dirs(yes) dir-group("news") dir-owner("news") dir-perm(0750)
suppress(30) owner(news) group(news)); };
log { source(src); source(chroots); filter(f_newscrit); destination(newscrit); };

destination newserr    { file("/var/log/news/news.err"
    create-dirs(yes) dir-group("news") dir-owner("news") dir-perm(0750)
suppress(30) owner(news) group(news)); };
log { source(src); source(chroots); filter(f_newserr); destination(newserr); };

destination newsnotice { file("/var/log/news/news.notice"
    create-dirs(yes) dir-group("news") dir-owner("news") dir-perm(0750)
suppress(30) owner(news) group(news)); };
log { source(src); source(chroots); filter(f_newsnotice); destination(newsnotice);
};
"
```

It seems to work fine. For the Tumbleweed / Leap route I'd go this direction and
remove the log file creation part completely, not just for news.

What do you think?

Johannes Segitz 2020-04-24 07:38:47 UTC

Comment 20

(In reply to peter czanik from comment #18)

> if [[-L var/log/news/news.err]]; then echo "oops, var/log/news/news.err is a sy

This is a TOCTOU vulnerabilty (https://en.wikipedia.org/wiki/Time-of-check_to_time-
of-use). If you check first and then act on this I can come in between the check
and the action.

You could package the var/log/news directory with the proper permissions (that
shouldn't cause issues with overwriting existing files and then use setpriv to
create the files as the news use if they don't exits. In this case the TOCTOU issue
isn't a problem since the news user can't gain additional privileges.

Thanks for the syslog-ng snipped, I'll have a look if this is secure

---

Thomas Blume 2020-04-30 04:56:44 UTC

Comment 21

(In reply to Johannes Segitz from comment #14)

> (In reply to Thomas Blume from comment #13)
> no that doesn't work as this would mean that root operates in a user
> controlled directory. That is really hard to do right and almost impossible
> in bash.
>
> Since %ghost doesn't work please give %config(noreplace) at try. Maybe
> someone with more packaging knowledge has a better idea

My tests confirm that this works.
If there are no objections, I will submit that for the SLES LTSS versions.
For openSUSE we can find a better approach but for LTSS, I guess it's the best we
can do.

Johannes Segitz 2020-04-30 07:46:00 UTC

Comment 22

(In reply to Thomas Blume from comment #21)
okay lets do that. In the meantime I had a look at the configuration example you
provided. First testing showed it to be secure, so that would be the way forward in
my opinion. I didn't have time for an in depth look though, maybe at a later time

---

Swamp Workflow Management 2020-05-07 19:28:17 UTC

Comment 25

SUSE-SU-2020:1221-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1169385
CVE References: CVE-2020-8019
Sources used:
SUSE Linux Enterprise Server for SAP 12-SP1 (src):   syslog-ng-3.6.4-12.8.1
SUSE Linux Enterprise Module for Legacy Software 12 (src):   syslog-ng-3.6.4-
12.8.1

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.

```
it to Base:System and Tumbleweed.

My other concern is, who could submit the fix to openSUSE Leap 15.1? I could not
find a workflow for it in the wiki, and probably it is easier for someone, who did
it a few times anyway.

(sorry for the late answer, since Monday I have troubles logging in)
```

Thomas Blume   2020-05-15 12:12:52 UTC

```
(In reply to peter czanik from comment #31)
> (In reply to Thomas Blume from comment #29)
> > Peter, what info do you need from me?
> > The changes look ok to me, but I'm not in the reviewers team for syslog-ng
> > on openSUSE.
>
> This is the main information I need. As in this case I can go ahead and and
> submit it to Base:System and Tumbleweed.
>
> My other concern is, who could submit the fix to openSUSE Leap 15.1? I could
> not find a workflow for it in the wiki, and probably it is easier for
> someone, who did it a few times anyway.

I can take care of this when the Tumbleweed request has been accepted.

> (sorry for the late answer, since Monday I have troubles logging in)

np. I wasn't sure whether you could see my comment, since it was initially set to
private.
```

peter czanik   2020-05-16 07:39:29 UTC

```
Thanks! It is now accepted: https://build.opensuse.org/request/show/805818
```

OBSbugzilla Bot   2020-05-20 08:10:08 UTC

```
This is an autogenerated message for OBS integration:
This bug (1169385) was mentioned in
https://build.opensuse.org/request/show/807465 15.1 / syslog-ng
```

Swamp Workflow Management   2020-05-23 16:12:43 UTC

```
openSUSE-RU-2020:0700-1: An update that has one recommended fix can now be
installed.

Category: recommended (moderate)
Bug References: 1169385
CVE References:
Sources used:
openSUSE Leap 15.1 (src):    syslog-ng-3.19.1-lp151.3.6.1
```

Swamp Workflow Management   2020-06-03 13:14:33 UTC

```
openSUSE-RU-2020:0761-1: An update that has one recommended fix can now be
installed.

Category: recommended (moderate)
Bug References: 1169385
CVE References:
Sources used:
openSUSE Backports SLE-15-SP1 (src):    syslog-ng-3.19.1-bp151.4.6.1
```

Wolfgang Frisch   2020-06-03 13:58:41 UTC

```
Released.
```