checkinstall adds local root exploits to any package with a symlink in it

Bug #1861281 reported by Gianni Tedesco on 2020-01-29

This bug affects 1 person

256

Affects	Status	Importance	Assigned to	Milestone
checkinstall (Ubuntu)	Confirmed	Undecided	Unassigned	

Bug Description

I create a tarball using the following script, it's a file, and a symlink to a file.

```
--8<---

#!/bin/sh

rm -rf usr/bin
mkdir -p usr/bin
echo -e '#!/bin/sh\necho Hi I am `id`' > usr/bin/writable
chmod 755 usr/bin/writable
ln -sf writable usr/bin/vulnerable
tar c usr/bin/writable usr/bin/vulnerable | gzip -c > pkg.tar.gz

--8<---
```

Then, I make untaring this file the subject of a checkinstall package:

```
checkinstall \
                --install=no \
                -d0 \
                -y \
                --pakdir=deb \
                --pkgname=vulnerable \
                --pkgversion=13.37 \
                --pkgrelease=1 \
                --nodoc \
                --deldesc=yes \
                --backup \
                -- \
  bash -c "gzip -cd pkg.tar.gz| (cd /; tar xv)"
```

Then I install this package with dpkg and end up with:

```
lrwxrwxrwx 1 gianni gianni 8 Jan 29 12:50 /usr/bin/vulnerable -> writable
-rwxrwxrwx 1 gianni gianni 31 Jan 29 12:50 /usr/bin/writable
```

Oh no, world writable binary, when the original was mode 755. Now a user can modify the contents and wait for root to run the command. Hey presto, local privlege execution and arbitrary code execution.

Looks like this is due to some fubar surround preservation of permissions vs symlinks.

Gianni Tedesco (scara) wrote on 2020-01-29: #1

A related bug, which I don't want to post separately because it's too close to this.

Is that when the tar creation has the symlink and the target in the opposite order, then checkinstall fails totally (note that the command being run works when NOT being run under checkinstall):

```
checkinstall 1.6.2, Copyright 2009 Felipe Eduardo Sanchez Diaz Duran
           This software is released under the GNU GPL.

*****************************************
**** Debian package creation selected ***
*****************************************

This package will be built according to these values:

0 - Maintainer: [ root@turf ]
1 - Summary: [ Package created with checkinstall 1.6.2 ]
2 - Name: [ vulnerable ]
3 - Version: [ 13.37 ]
4 - Release: [ 2 ]
5 - License: [ GPL ]
6 - Group: [ checkinstall ]
7 - Architecture: [ amd64 ]
8 - Source location: [ checkpwn ]
9 - Alternate source location: [ ]
10 - Requires: [ ]
11 - Provides: [ vulnerable ]
12 - Conflicts: [ ]
13 - Replaces: [ ]

Enter a number to change any of them or press ENTER to continue:

Installing with bash -c gzip -cd rev.tar.gz| (cd /; tar xv)...

========================= Installation results ===========================
usr/bin/vulnerable
tar: usr/bin/vulnerable: Cannot change mode to rwxrwxrwx: No such file or
directory
usr/bin/writable
tar: Exiting with failure status due to previous errors

**** Installation failed. Aborting package creation.

Cleaning up...OK

Bye.
```

summary:- checkinstall may add local root exploits to packages with symlinks in
- them

Report a bug

This report contains **Public Security** information

Everyone can see this security related information.

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

Gianni Tedesco

May be notified

Alejandro J. Alva...
Ashani Holland
Bruno Garcia
CRC
Charlie_Smotherman
Debian PTS
Doraann2
Franko Fang
HaySayCheese
Hidagawa
Jesse Jones
José Alfonso
Matt j
Mr. MInhaj
Name Changed
PCTeacher012
Paolo Topa
Peter Bullert
Punnsa
Richard Seguin
Richard Williams
Stephen Gelman
Tom Weiss
Ubuntu Security Team
Vasanth
Vic Parker
ahepas
basilisgabri
dsfkj dfjx
eoininmoran
ganesh
linuxgijs
nikonikic42
projevie@hotmail.com
qadir
sankaran
van

```
        + checkinstall adds local root exploits to any package with a symlink in
        + it
```

Seth Arnold (seth-arnold) wrote on 2020-02-04: #2

Hello, nice writeup and reproducer; have you reported these issues upstream yet?

Thanks

information type:Private Security → Public Security

Gianni Tedesco (scara) wrote on 2020-02-05: #3

Ah no, the upstream link I found on launchpad was dead but I think I know what to do with it now.

Gianni Tedesco (scara) wrote on 2020-02-05: #4

Welp, their bugtracker is dead and I wasn't sure about how appropriate the mailing list would be

Gianni Tedesco (scara) wrote on 2020-02-05: #5

Sent an email to the maintainer

Stephen Gelman (ssgelm) wrote on 2020-02-05: #6

Hi!

I am the Debian maintainer of checkinstall. As you have noticed the upstream appears to be pretty dead. I've tried to contact the original author about the bug tracker being down and have never received a reply. I will see what I can do to fix the security issues you reported in the Debian package which will then be pulled into Ubuntu.

Thanks,

Stephen

Seth Arnold (seth-arnold) wrote on 2020-02-06: #7

Hello Stephen, pity the original authors have moved on, but I can understand. Thanks for giving this a look.

Thanks

Marc Deslauriers (mdeslaur) on 2020-03-11

Changed in checkinstall (Ubuntu):
  status:New → Confirmed

See full activity log

To post a comment you must log in.