~~Bug 1182166 - (CVE-2021-25314) VUL-0: CVE-2021-25314: hawk2: Insecure file permissions~~

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: Stefano Torresi
QA Contact: Security Team bot

URL: https://smash.suse.de/issue/277858/
Whiteboard: CVSSv3.1:SUSE:CVE-2021-25314:8.4:(AV:...
Keywords:

Depends on:
Blocks: 1180004
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2021-02-12 08:53 UTC by Johannes Segitz
Modified: 2022-08-11 08:43 UTC (History)
CC List: 11 users (show)

See Also:
Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Flags: gianluca.gabrielli: needinfo? (aburlakov)

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 2021-02-12 08:53:26 UTC Description

```
+++ This bug was initially created as a clone of Bug #1180004 +++

3, Insecure file permissions
In three different places you set files to unsafe permissions
- hawk/app/models/report.rb
  147     File.chmod(0666, tmpfile.path)
  Only used to generates graph, shouldn't be more than a DoS that someone
  that can abuse this cause likely via other vectors.
- hawk/app/lib/invoker.rb
  69       File.chmod(0666, f.path)
  70       CrmEvents.instance.push "crm configure\n#{cmd}\n" unless @no_log
  71       result = crm '-F', 'configure', 'load', 'update', f.path
  This allows arbitrary local users to change the CIB, which is an issue in
  itself, but can be combined with other issues, e.g. 2 to set uname to
  something containing shell metacharacters.
- hawk/app/lib/crm_script.rb
  42   def run(jsondata, rootpw)
  43     user = current_user
  44     cmd = crmsh_escape(JSON.dump(jsondata))
  45     tmpf = Tempfile.new 'crmscript'
  46     tmpf.write("script json \"#{cmd}\"")
  47     tmpf.close
  48     File.chmod(0666, tmpf.path)
  49
  50     if rootpw.nil?
  51       cmdline = ['/usr/sbin/hawk_invoke', user, 'crm', '-f', tmpf.path]
  52     else
  53       user = 'root'
  54       cmdline = ['/usr/bin/su', user, '--shell=/bin/sh', '-c', "/usr/sbin/crm
-f #{tmpf.path}", stdin_data: rootpw.lines.first]
  55     end
  56     old_home = Util.ensure_home_for(user)
  57     out, err, status = Util.capture3(*cmdline)
  The last one is a root exploit as crm is powerful and can be misused in
  various ways

My suggestion is that you don't change the permissions here. I've seen in
the comments that you considered doing this anyway
```

Johannes Segitz 2021-02-12 08:55:06 UTC Comment 1

```
This is an embargoed bug. This means that this information is not public.
CRD: 2021-05-13 (or earlier, internal finding)

Please do NOT:
- talk to other people about this unless they're involved in fixing the issue
- make this bug public
- submit this into OBS (e.g. fix Leap/Tumbleweed) until this bug becomes public
(e.g. no EMBARGOED tag on the header)

Consult with security team if you think that the issue is public and the bug is
still private (e.g. subject still contains "EMBARGOED"). Please do NOT make the bug
public yourself.

Please be aware that the SUSE:SLE-15-SP3:GA codestream is available via OBS, so do
NOT submit there before this is public.

These are the steps that are asked from you:
1, Your primary responsibility is to submit a fix for this issue. Here's a how-to
for submitting packages for maintenance releases in IBS:

https://confluence.suse.com/display/maintenance/How+to+Submit+Packages+or+Containers+
   Apart from the GA codestreams mentioned above, you can submit to IBS anytime.
This is private and allows us to start testing as soon as possible.
```

2, We also want to fix openSUSE if it's affected.
   $ is_maintained $PACKAGE
   will tell you if the package is inherited from SLES or if it is branched for openSUSE. There are two cases:
   - It's coming from SLES: The update will automatically be released for openSUSE. Nothing to do for you.
   - It's branched for openSUSE: You need to submit AFTER the bug became public, to the current openSUSE codestreams.
   For openSUSE Factory please submit to the devel project of you package AFTER the bug became public.

Security will then take the following steps:
- We wait for your submission and package them into an incident for QA testing. The QA tester might reach out to you if they find issues with the update.
- Once the coordinated release date (CRD), the date this issue should become public, is reached (or for internal findings: once we're done testing), we remove the EMBARGOED tag from this bug and publish the updates.
- Only if the bug here is public you may submit to public repositories (OBS).

You can contact us at:

* IRC: irc.suse.de #security
* RocketChat: https://chat.suse.de/channel/security
* Email: security-team@suse.de

Comment 3

fixed my next 2.6.3 mu

Alexandros Toptsoglou 2021-03-15 10:47:03 UTC Comment 6

Do we have a CRD or should we release when we have ready most of the codestreams?

Johannes Segitz 2021-03-18 09:51:24 UTC Comment 8

(In reply to Alexandros Toptsoglou from comment #6)
we can release whenever we like, no external CRD

Johannes Segitz 2021-03-24 12:30:26 UTC Comment 10

Update was released

Comment 11

SUSE-SU-2021:0941-1: An update that solves two vulnerabilities and has one errata is now available.

Category: security (important)
Bug References: 1179999,1182165,1182166
CVE References: CVE-2020-35459,CVE-2021-25314
JIRA References:
Sources used:
SUSE Linux Enterprise High Availability 15-SP2 (src):   hawk2-2.6.3+git.1614684118.af555ad9-3.27.1
SUSE Linux Enterprise High Availability 15-SP1 (src):   hawk2-2.6.3+git.1614684118.af555ad9-3.27.1
SUSE Linux Enterprise High Availability 15 (src):   hawk2-2.6.3+git.1614684118.af555ad9-3.27.1

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 2021-03-24 14:28:30 UTC Comment 12

SUSE-SU-2021:0942-1: An update that solves two vulnerabilities and has one errata is now available.

Category: security (important)
Bug References: 1179999,1182165,1182166
CVE References: CVE-2020-35459,CVE-2021-25314
JIRA References:
Sources used:
SUSE Linux Enterprise High Availability 12-SP5 (src):   hawk2-2.6.3+git.1614685906.812c31e9-3.30.1
SUSE Linux Enterprise High Availability 12-SP4 (src):   hawk2-2.6.3+git.1614685906.812c31e9-3.30.1

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 2021-03-24 14:37:29 UTC Comment 13

SUSE-SU-2021:0943-1: An update that solves two vulnerabilities and has one errata is now available.

Category: security (important)
Bug References: 1179999,1182165,1182166
CVE References: CVE-2020-35459,CVE-2021-25314
JIRA References:
Sources used:
SUSE Linux Enterprise High Availability 12-SP3 (src):   hawk2-2.6.3+git.1614685906.812c31e9-2.42.1

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.

Aleksei Burlakov 2022-04-13 13:06:32 UTC Comment 17

Hi Johannes Segitz, I have submitted the patch to the factory.
https://api.opensuse.org/request/show/967820
Can we close the ticket?

Aleksei Burlakov 2022-04-19 13:24:59 UTC Comment 18

The patch was submitted to the factory.
https://api.opensuse.org/request/show/967820

Johannes Segitz 2022-04-26 07:26:15 UTC Comment 19

(In reply to Aleksei Burlakov from comment #17)
yes (it's already closed)
