Bug 1182321 - (CVE-2021-31998) VUL-0: CVE-2021-31998: inn: %post calls user owned file, LPE to root

Status:	NEW
Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Incidents
Version:	unspecified
Hardware:	Other Other
Priority:	P3 - Medium **Severity**: Normal
Target Milestone:	---
Assigned To:	Michael Schröder
QA Contact:	Security Team bot
URL:	
Whiteboard:	CVSSv3.1:SUSE:CVE-2021-31998:7.3:(AV:...
Keywords:	
Depends on:	
Blocks:	
	Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2021-02-16 13:03 UTC by Johannes Segitz
Modified:	2021-07-08 19:30 UTC (History)
CC List:	2 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.

Johannes Segitz 2021-02-16 13:03:55 UTC Description

```
284 if test -e %{nslash}/news/bin/control/version -o -e %
{nslash}/news/bin/inndstart ; then
285     rm -f etc/news/inn.conf.OLD
286     rm -f etc/news/newsfeeds.OLD
287     %{nslash}rnews/bin/innupgrade etc/news
288 fi

innupgrade belongs to root
-r-xr-x---. 1 news news system_u:object_r:bin_t:s0 12K Feb 11 22:40
/usr/lib/news/bin/innupgrade

I assume that's some migration code, because on my system the if clause is false
since both files don't exist.

Is there a reason why the files in /usr/lib/news/bin/ belong to news? I remember we
had a similar issue a while ago
```

Johannes Segitz 2021-02-16 13:04:52 UTC Comment 1

```
This is an embargoed bug. This means that this information is not public.

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

CRD: 2021-05-17 or earlier, internal finding

Comment 2

It's somewhat historic. The binaries that can be called by any user have mode 755, others that are only useful to the inn server have owner:group news:news and mode 750.

Seems like that innupgrade command should not be called by user root, but user news instead.

Michael Schröder 2021-03-05 13:41:26 UTC Comment 3

Is there a CVE for this?

Marcus Meissner 2021-05-20 11:30:56 UTC Comment 4

can you assign a CVE?

Johannes Segitz 2021-05-20 14:57:57 UTC Comment 5

Please use CVE-2021-31998 for this

OBSbugzilla Bot 2021-05-31 12:30:03 UTC Comment 7

```
This is an autogenerated message for OBS integration:
This bug (1182321) was mentioned in
https://build.opensuse.org/request/show/896351 15.2 / inn
https://build.opensuse.org/request/show/896352 Backports:SLE-15-SP3 / inn
```

Swamp Workflow Management 2021-06-03 19:16:12 UTC Comment 8

```
openSUSE-SU-2021:0830-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1182321
CVE References: CVE-2021-31998
JIRA References:
Sources used:
openSUSE Leap 15.2 (src):    inn-2.6.2-lp152.2.6.1
```

Swamp Workflow Management 2021-06-07 01:16:57 UTC Comment 9

```
openSUSE-SU-2021:0845-1: An update that fixes one vulnerability is now available.

Category: security (moderate)
Bug References: 1182321
CVE References: CVE-2021-31998
JIRA References:
Sources used:
openSUSE Backports SLE-15-SP2 (src):    inn-2.6.2-bp152.2.8.1
```

Swamp Workflow Management 2021-06-17 13:17:22 UTC Comment 12

```
SUSE-SU-2021:14750-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1182321
CVE References: CVE-2021-31998
JIRA References:
Sources used:
SUSE Linux Enterprise Server 11-SP4-LTSS (src):    inn-2.4.2-170.21.3.6.1
SUSE Linux Enterprise Point of Sale 11-SP3 (src):    inn-2.4.2-170.21.3.6.1
SUSE Linux Enterprise Debuginfo 11-SP4 (src):    inn-2.4.2-170.21.3.6.1
SUSE Linux Enterprise Debuginfo 11-SP3 (src):    inn-2.4.2-170.21.3.6.1

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 2021-07-08 19:30:32 UTC Comment 13

```
openSUSE-SU-2021:0986-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1182321
CVE References: CVE-2021-31998
JIRA References:
Sources used:
openSUSE Backports SLE-15-SP3 (src):    inn-2.6.2-bp153.3.3.1
```

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

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