~~Bug 1186240 - (CVE-2021-25321) VUL-0: CVE-2021-25321: arpwatch: LPE from runtime user to root~~

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:	Johannes Segitz
QA Contact:	Security Team bot
URL:	
Whiteboard:	CVSSv3.1:SUSE:CVE-2021-25321:7.7:(AV:...
Keywords:	
Depends on:	
Blocks:	

Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2021-05-19 11:25 UTC by Johannes Segitz
Modified:	2021-07-11 10:19 UTC (History)
CC List:	1 user (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 2021-05-19 11:25:35 UTC Description

```
while preparing the first major update I noticed this while rebasing the existing
patches.

/var/lib/arpwatch is packaged as root:root. Once arpwatch was run with a
unprivileged user the ownership is changed to the unprivileged user

$ arpwatch -u johannes -d
$ ls -lad /var/lib/arpwatch
drwxr-xr-x 2 johannes users 4096 May 19 13:18 /var/lib/arpwatch

arpwatch-2.1a11-drop-privs.dif adds a "droppriveleges" function that does this
+               if ( chown ( arpfile, pw->pw_uid, pw->pw_gid) != 0 ||
+                       chown ( arpfiledir, pw->pw_uid, pw->pw_gid) != 0  ) {
+                       syslog(LOG_ERR, "Fatal: could not chown %s and %s to
%d,%d).",
+                               arpfiledir,arpfile, pw->pw_uid, pw->pw_gid);
+                       exit(1);
+               }

which allows the user specified to escalate to root the next time arpwatch is
started.

As user:
# id
uid=1000(johannes) gid=100(users) groups=100(users)
# pwd
/var/lib/arpwatch
# rm arp.dat
# ln -s /etc/shadow arp.dat

Start arpwatch again, after that /etc/shadow is owned by johannes
-rw-r----- 1 johannes users 1.3K May 17 17:08 /etc/shadow
```

Johannes Segitz 2021-06-11 11:58:35 UTC Comment 3

```
I have a patch that I'm testing and will likely submit today to maintenance
```

Robert Frohl 2021-06-28 13:47:26 UTC Comment 5

```
public via SUSE release
```

Swamp Workflow Management 2021-06-28 19:18:50 UTC Comment 6

```
SUSE-SU-2021:14759-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1186240
CVE References: CVE-2021-25321
JIRA References:
Sources used:
SUSE Linux Enterprise Server 11-SP4-LTSS (src):    arpwatch-2.1a15-131.23.2.6.1
SUSE Linux Enterprise Point of Sale 11-SP3 (src):    arpwatch-2.1a15-131.23.2.6.1
SUSE Linux Enterprise Debuginfo 11-SP4 (src):    arpwatch-2.1a15-131.23.2.6.1
SUSE Linux Enterprise Debuginfo 11-SP3 (src):    arpwatch-2.1a15-131.23.2.6.1

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 2021-06-28 19:45:19 UTC Comment 7

```
SUSE-SU-2021:2175-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1186240
CVE References: CVE-2021-25321
JIRA References:
Sources used:
SUSE OpenStack Cloud Crowbar 9 (src):    arpwatch-2.1a15-159.9.1
SUSE OpenStack Cloud Crowbar 8 (src):    arpwatch-2.1a15-159.9.1
SUSE OpenStack Cloud 9 (src):    arpwatch-2.1a15-159.9.1
SUSE OpenStack Cloud 8 (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Software Development Kit 12-SP5 (src):    arpwatch-2.1a15-
159.9.1
SUSE Linux Enterprise Server for SAP 12-SP4 (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Server for SAP 12-SP3 (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Server 12-SP5 (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Server 12-SP4-LTSS (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Server 12-SP3-LTSS (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Server 12-SP3-BCL (src):    arpwatch-2.1a15-159.9.1
SUSE Linux Enterprise Server 12-SP2-BCL (src):    arpwatch-2.1a15-159.9.1
HPE Helion Openstack 8 (src):    arpwatch-2.1a15-159.9.1

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 2021-06-28 20:10:22 UTC Comment 8

```
SUSE-SU-2021:2177-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1186240
CVE References: CVE-2021-25321
JIRA References:
Sources used:
SUSE Manager Server 4.0 (src):    arpwatch-2.1a15-5.12.1
SUSE Manager Retail Branch Server 4.0 (src):    arpwatch-2.1a15-5.12.1
SUSE Manager Proxy 4.0 (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Server for SAP 15-SP1 (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Server for SAP 15 (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Server 15-SP1-LTSS (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Server 15-SP1-BCL (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Server 15-LTSS (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Module for Basesystem 15-SP3 (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise Module for Basesystem 15-SP2 (src):    arpwatch-2.1a15-5.12.1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS (src):    arpwatch-
2.1a15-5.12.1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS (src):    arpwatch-
2.1a15-5.12.1
SUSE Linux Enterprise High Performance Computing 15-LTSS (src):    arpwatch-2.1a15-
5.12.1
SUSE Linux Enterprise High Performance Computing 15-ESPOS (src):    arpwatch-
2.1a15-5.12.1
SUSE Enterprise Storage 6 (src):    arpwatch-2.1a15-5.12.1
SUSE CaaS Platform 4.0 (src):    arpwatch-2.1a15-5.12.1

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 2021-07-01 10:15:56 UTC Comment 9

```
openSUSE-SU-2021:0945-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1186240
CVE References: CVE-2021-25321
JIRA References:
Sources used:
openSUSE Leap 15.2 (src):    arpwatch-2.1a15-lp152.6.9.1
```

Johannes Segitz 2021-07-05 07:13:19 UTC Comment 10

```
all updates submitted
```

Swamp Workflow Management 2021-07-11 10:19:36 UTC Comment 11

```
openSUSE-SU-2021:2177-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1186240
CVE References: CVE-2021-25321
JIRA References:
Sources used:
openSUSE Leap 15.3 (src):    arpwatch-2.1a15-5.12.1
```