lathiat / avahi Public

New issue

Jump to bottom

reachable assertion in avahi_s_host_name_resolver_start when trying to resolve badly-formatted hostnames (CVE-2021-3502) #338

Closed carnil opened this issue on Apr 26, 2021 · 2 comments

Milestone v0.9

carnil commented on Apr 26, 2021

Hi

An issue was reported in Debian as https://bugs.debian.org/986018 which got CVE-2021-3502 assigned. Quoting the report:

```
Package: avahi-daemon
Version: 0.8-5
Severity: important
Tags: security
Control: notfound -1 0.7-4+b1

Dear Maintainers,

I found another local denial-of-service vulnerability in avahi-daemon.
It can be triggered by trying to resolve badly-formatted hostnames on
the /run/avahi-daemon/socket interface (I stumbled upon it, accidentally
trying to resolve an IP as a hostname...)
This time the daemon just dies, and this time buster is not affected.

Steps to reproduce:
  $ (echo "RESOLVE-HOSTNAME a"; sleep 3;) | socat - /run/avahi-daemon/socket
  $ ps -FC avahi-daemon

Same results for these queries: "a.", ".a", "a..b", ".b.c", "a.b.."

Note that every local user has access to the socket.


Yours
Thomas Kremer
```

carnil changed the title ~~eachable assertion in avahi_s_host_name_resolver_start when trying to resolve badly-formatted hostnames (CVE-2021-3502)~~ reachable assertion in avahi_s_host_name_resolver_start when trying to resolve badly-formatted hostnames (CVE-2021-3502) on Apr 26, 2021

carnil commented on Apr 26, 2021 Author

Additional downstream reference: https://bugzilla.redhat.com/show_bug.cgi?id=1946914

rantala commented on Apr 27, 2021 Contributor

Hi,

Based on quick testing this PR fixes it, can you also try it and confirm?
#324

lathiat closed this as completed in `fd482a7` on Jun 4, 2021

lathiat added this to the **v0.9** milestone on Jun 4, 2021

evverx mentioned this issue 2 weeks ago

Emit error if Dbus requested service is not found #407

Open

evverx added a commit to evverx/avahi that referenced this issue 2 weeks ago

`CI: bring radamsa` ··· ✗ `8d864ff`

evverx added a commit to evverx/avahi that referenced this issue 2 weeks ago

`CI: bring radamsa` ··· ✗ `1bef1b6`

evverx added a commit to evverx/avahi that referenced this issue 2 weeks ago

`CI: bring radamsa` ··· ✗ `f382cbe`

evverx added a commit to evverx/avahi that referenced this issue 2 weeks ago

`CI: bring radamsa` … ✗ `54d6e1c`

evverx added a commit to evverx/avahi that referenced this issue 2 weeks ago

`CI: bring radamsa` … ✗ `d51a131`

evverx added a commit to evverx/avahi that referenced this issue 2 weeks ago

`CI: bring radamsa` … ✗ `c660f88`

evverx mentioned this issue 2 weeks ago

Need some checks run on each PR #412

⊙ Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

v0.9

Development

No branches or pull requests

3 participants