Bug 1946914 (CVE-2021-3502) - CVE-2021-3502 avahi: reachable assertion in avahi_s_host_name_resolver_start when trying to resolve badly-formatted hostnames

Keywords: Security ×

Status: CLOSED NOTABUG
Alias: CVE-2021-3502
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Duplicates (1): ~~CVE-2021-36217~~ (view as bug list)
Depends On: 1949949 ~~1946916~~
Blocks: 1946920 1950126 1989383
TreeView+ depends on / blocked

Reported: 2021-04-07 08:57 UTC by Marian Rehak
Modified: 2021-10-28 12:23 UTC (History)
CC List: 6 users (show)
Fixed In Version:
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in avahi. A reachable assertion is present in avahi_s_host_name_resolver_start function allowing a local attacker to crash the avahi service by requesting hostname resolutions through the avahi socket or dbus methods for invalid hostnames. The highest threat from this vulnerability is to the service availability.
Clone Of:
Environment:
Last Closed: 2021-10-28 12:23:47 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Marian Rehak 2021-04-07 08:57:22 UTC — Description

A local Dos in avahi-daemon that can be triggered by trying to resolve badly-formatted hostnames on the /run/avahi-daemon/socket interface.

References:

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=986018

Marian Rehak 2021-04-07 08:58:45 UTC — Comment 1

Created avahi tracking bugs for this issue:

Affects: fedora-all [~~bug 1946915~~]

~~inecchen~~ 2021-04-08 12:12:43 UTC — Comment 2

The avahi-daemon Linux service runs on client machines to perform network-based Zeroconf service discovery. Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zeroconf Networking.

avahi running on the client machine, this may affect the openshift product but no the services

~~Riccardo Schirone~~ 2021-04-15 12:45:59 UTC — Comment 3

Function avahi_s_host_name_resolver_start() in resolve-host-name.c:

```
void avahi_s_host_name_resolver_start(AvahiSHostNameResolver *r) {
    assert(r);

    if(r->record_browser_a)
        avahi_s_record_browser_start_query(r->record_browser_a);

    if(r->record_browser_aaaa)
        avahi_s_record_browser_start_query(r->record_browser_aaaa);
}
```

The assert(r) may trigger when a user pass to RESOLVE-HOSTNAME functionality in /run/avahi-daemon/socket an invalid hostname. Invalid hostnames are determined through function avahi_is_valid_fqdn() in domain.c.

~~Riccardo Schirone~~ 2021-04-15 13:01:55 UTC — Comment 4

In reply to comment #3:
> The assert(r) may trigger when a user pass to RESOLVE-HOSTNAME functionality
> in /run/avahi-daemon/socket an invalid hostname. Invalid hostnames are
> determined through function avahi_is_valid_fqdn() in domain.c.

The issue can be triggered even through dbus method org.freedesktop.Avahi.Server.ResolveHostName.

~~Riccardo Schirone~~ 2021-04-15 13:02:46 UTC — Comment 5

If assertions are compiled out, this issue would result in a NULL pointer dereference, which would still constitute a local Denial of Service against the Avahi service.

~~Riccardo Schirone~~ 2021-04-15 13:04:36 UTC — Comment 6

The vulnerability was introduced in upstream commit https://github.com/lathiat/avahi/commit/80c98fa16782e921f5b5d5c880f1d80f5c43bd49, which was shipped with upstream version 0.8.

~~Riccardo Schirone~~ 2021-04-15 13:14:22 UTC Comment 8

Statement:

This issue did not affect the versions of avahi as shipped with Red Hat Enterprise Linux 6, 7, and 8 as they did not include the vulnerable code.

Salvatore Bonaccorso 2021-04-16 06:56:41 UTC Comment 11

Has this been reported upstream?

Marian Rehak 2021-04-26 14:22:19 UTC Comment 12

@Salvatore No report upstream by me.

Salvatore Bonaccorso 2021-04-26 17:06:45 UTC Comment 13

(In reply to Marian Rehak from comment #12)
> @Salvatore No report upstream by me.

Okay, I filled a report here https://github.com/lathiat/avahi/issues/338

Garrett Tucker 2021-08-09 16:51:09 UTC Comment 14

*** ~~Bug 1989301~~ has been marked as a duplicate of this bug. ***

Note
You need to log in before you can comment on or make changes to this bug.