home-assistant / plugin-dns Public

Code   Issues 4   Pull requests 1   Actions   Security   Insights

New issue

Jump to bottom

Home Assistant OS leaks private host names to cloudflare DNS service (CVE-2020-36517) #70

Closed **mtdcr** opened this issue on Jan 15 · 10 comments · Fixed by #86

mtdcr commented on Jan 15

Describe the issue you are experiencing

Home Assistant OS always gets configured to load-balance between my DNS resolver and Cloudflare's. I already looked under every stone, but there's no way to disable this behavior using configuration options.

So if I use DNS names configured by my router instead of hard-coding IP addresses, HA will switch over to Cloudflare from time to time and leak my internal hostnames to their service. Of course resolution fails in this case, too. Note that this is not caused by the hard-coded fallback option, but by the hard-coded load-balancing option.

One way to avoid this could be blocking 1.1.1.1 and 1.0.0.1 in my firewall, but then HA's DNS resolver goes berserk flooding my firewall logs with multiple connection attempts per second. Also, this will break further whenever developers decide to switch their user base from Cloudflare to a new data collection service.

What operating system image do you use?

ova (for Virtual Machines)

What version of Home Assistant Operating System is installed?

7.1

Did you upgrade the Operating System.

Yes

Steps to reproduce the issue

1. Insert local hostname in HA config
2. Notice recurring failures in name resolution
3. Notice packets going to 1.0.0.1 and 1.1.1.1

Anything in the Supervisor logs that might be useful for us?

```
-
```

Anything in the Host logs that might be useful for us?

```
Typical output of `ha dns log` when the service gets blocked.
~~~
[INFO] 127.0.0.1:44130 - 10230 "NS IN . udp 17 false 512" NOERROR - 0 30.001023101s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
[INFO] 127.0.0.1:51517 - 36166 "NS IN . udp 17 false 512" NOERROR - 0 30.000661016s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:34985 - 13557 "NS IN . udp 17 false 512" NOERROR - 0 30.001216215s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:39902 - 40031 "NS IN . udp 17 false 512" NOERROR - 0 30.000821668s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
[INFO] 127.0.0.1:43380 - 37784 "NS IN . udp 17 false 512" NOERROR - 0 30.000649803s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:60231 - 1526 "NS IN . udp 17 false 512" NOERROR - 0 30.000941436s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:42409 - 17159 "NS IN . udp 17 false 512" NOERROR - 0 30.001298402s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
[INFO] 127.0.0.1:37011 - 7485 "NS IN . udp 17 false 512" NOERROR - 0 30.00056859s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:46069 - 34633 "NS IN . udp 17 false 512" NOERROR - 0 30.001109111s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:52199 - 55341 "NS IN . udp 17 false 512" NOERROR - 0 30.000769912s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:44575 - 61374 "NS IN . udp 17 false 512" NOERROR - 0 30.000521003s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
[INFO] 127.0.0.1:59716 - 56622 "NS IN . udp 17 false 512" NOERROR - 0 30.001314379s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
[INFO] 127.0.0.1:43202 - 11517 "NS IN . udp 17 false 512" NOERROR - 0 30.000960835s
[ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
~~~
```

System Health information

No response

Additional information

No response

👍 6

→ **agners** transferred this issue from home-assistant/operating-system on Jan 15

tic226n commented on Jan 16 • edited

I have (like many others[0]) the same problem. I noticed my firewall logs being flooded with DNS lookups to cloudflare servers. This is just bad design and quite frankly, it is ridiculous. The usual workaround of creating a dedicated block rule for the hardcoded cloudflare servers prevents entries being added to the logs and works well enough. Shame on the hass.io developers for ignoring this issue.

Edit: To make this 'future' proof i created an inverted block rule that blocks every DNS query from the HA host (53/853) that is *not* directed at my local DNS server.

[0] https://community.home-assistant.io/t/local-dns/178108/85

philipflesher commented on Feb 7

+1 -- same issue.

1 similar comment

alexiri mentioned this issue on Feb 23

Connections to Cloudflare DNS home-assistant/core#66482

Closed

mschilt commented on Feb 23

same issue here..
would be great if HA would only use the configured, internal DNS Server and not ping out to Cloudflare.
As far as I understood this is part of some kind of failback mechanism. I think that mechanism is probably not working correctly since my local DNS Service never has availability issues.

liudab commented on Feb 23

Same issue here, and there are numerous attempts to dial 1.0.0.1:853 and 1.1.1.1:853.
I tried to had edited /usr/share/hassio/dns.json and /usr/share/hassio/dns/coredns.json, not help with issue, and this issue slowed down my local network.
Pls fix this issue, and let users choose.

```
Feb 24 10:29:33 raspberrypi c25c8d59d674[766]: [ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
Feb 24 10:29:35 raspberrypi c25c8d59d674[766]: [INFO] 127.0.0.1:43745 - 14836 "NS IN . udp 17 false 512" NOERROR - 0 30.001163805s
Feb 24 10:29:35 raspberrypi c25c8d59d674[766]: [ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
Feb 24 10:29:36 raspberrypi c25c8d59d674[766]: [INFO] 127.0.0.1:43857 - 18263 "NS IN . udp 17 false 512" NOERROR - 0 30.000670555s
Feb 24 10:29:36 raspberrypi c25c8d59d674[766]: [ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
Feb 24 10:29:38 raspberrypi c25c8d59d674[766]: [INFO] 127.0.0.1:46192 - 23166 "NS IN . udp 17 false 512" NOERROR - 0 30.000614263s
Feb 24 10:29:38 raspberrypi c25c8d59d674[766]: [ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
Feb 24 10:29:39 raspberrypi c25c8d59d674[766]: [INFO] 127.0.0.1:41931 - 46048 "NS IN . udp 17 false 512" NOERROR - 0 30.000839356s
Feb 24 10:29:39 raspberrypi c25c8d59d674[766]: [ERROR] plugin/errors: 2 . NS: dial tcp 1.1.1.1:853: i/o timeout
Feb 24 10:29:41 raspberrypi c25c8d59d674[766]: [INFO] 127.0.0.1:54422 - 21526 "NS IN . udp 17 false 512" NOERROR - 0 30.00059314s
Feb 24 10:29:41 raspberrypi c25c8d59d674[766]: [ERROR] plugin/errors: 2 . NS: dial tcp 1.0.0.1:853: i/o timeout
```

hermanops commented on Feb 27

+1 -- same issue.

jaytea33 commented on Mar 4 • edited

There are tons of threads on this problem and the devs continue to ignore it. I don't think functioning DNS is an unreasonable request

https://community.home-assistant.io/t/ha-os-dns-setting-configuration-not-respected/356572/12

UPDATE: So the gist of it is this - don't count on this issue getting fixed any time soon or possibly ever. Dev's position is that prior to implementing this unholy bastardization of DNS, they had tons of support issues due to user DNS misconfigurations. So they issued a forced DNS fallback to ensure they don't waste their time troubleshooting it, and it's been great for them in their cozy ivory tower while users who actually understand how DNS is supposed to work are left to bash our heads trying to get around this downright abysmal implementation. I expect this behavior from Chinese IoT devices - not an open source project.

For many of us, the whole point of using HA is to localize everything as MUCH as possible! Clearly, there are some philosophical differences at work here, and it just ends up with threads either being locked or the issue ignored/going stale, then being bumped by justifiably frustrated users to no avail. This seems like much more of a corporate direction (maybe because Nabu Casa is the focus?), and if it keeps up, I can only hope someone with more development skills than I can fork HA to a build that prioritizes local IoT, security, non-retarded DNS, and embraces the open-source philosophy of user control and choice, similar to the Emby/Jellyfin treatment when Emby became corporate and unusable.

Anyway, rant over, time for the solution that so far seems to work for me:

Use this add-on to remove the forced fallback (among other things for advanced users):

https://github.com/bentasker/HomeAssistantAddons/tree/master/core-dns-override

While I'm not sure if both are necessary, I also used the AdGuard solution at the bottom of this page:

https://community.home-assistant.io/t/dns-configuration-help/182258/10

Just make sure to follow the instructions correctly for setting up AdGuard - it feels weird setting the HA Host to use a static Public DNS IP but the Upstream DNS configuration makes sense.

One thing to note though, after making any change in DNS, whether changing the HA Host's DNS IP or changing something in AdGuard, I've noticed that I have to restart the "Core DNS Override" addon, and then it reflects the new DNS config immediately (I'm assuming because it restarts the Core DNS service?).

Using the AdGuard setup instructions, you can easily add your local domain by configuring the Upstream DNS - just follow the examples below the fields, they're very clear. Then restart "Core DNS Override" addon and try nslookup against your local domain to verify it resolves.

The last piece I had to figure out was redirecting my *duckdns.org name to my local HA IP. This was previously handled by my router (which then points to NGINX Proxy Manager in HA) and for devices outside HA, it resolves locally just fine, so entering in with fake, redirected SSL still worked. But from HA's perspective, it's still looking at my Public IP when using nslookup against my *duckdns.org name. It turns out the fix is simple even though it took me a while to find:

In AdGuard, go to "Filters > DNS Rewrites > click "Add DNS rewrite" - then it's just like a classic hostfile edit at that point. Commit it, restart "Core DNS Override" again.

Hopefully this helps someone else struggling with these DNS issues (or devs decide to listen and we get a proper fix, but not holding my breath).

👍 2

mtdcr commented on Mar 6 Author

There's a CVE ID for this issue now: CVE-2020-36517.

👍 5

mtdcr changed the title ~~Home Assistant OS leaks private host names to cloudflare DNS service~~ Home Assistant OS leaks private host names to cloudflare DNS service (CVE-2020-36517) on Mar 6

hermanops commented on Mar 6

my firewall reports over 20.000 dns-leaks per minute to Cloudflare on port 853

mdegat01 mentioned this issue on Apr 21

No SERVFAIL and no forwarding multicast names #86

Merged

pvizeli closed this as completed in #86 on Apr 25

mdegat01 commented on Apr 25 • edited Contributor

Just an FYI for everyone, I believe #85 actually fixes most of the issues identified here since MDNS and LLMNR names are no longer forwarded to external resolvers. That covers everything except local hostnames that aren't MDNS and LLMNR. There is a follow-up PR to add an option to disable the fallback DNS here: home-assistant/supervisor#3586 . That should finish this out and allow you to stop those from being forwarded as well.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

No SERVFAIL and no forwarding multicast names
home-assistant/plugin-dns

9 participants