

New issue

[Jump to bottom](#)

turn: block forwarding to loopback/any #7

Merged arianvp merged 9 commits into master from block_local_any on Mar 12, 2021

Conversation 8 Commits 9 Checks 1 Files changed 8



z-dule commented on Mar 11, 2021

Contributor

No description provided.

turn: block forwarding to loopback/any

✓ ffa2d56



julialongtin reviewed on Mar 11, 2021

[View changes](#)

modules/turn/turn.c Outdated

Show resolved



julialongtin approved these changes on Mar 11, 2021

[View changes](#)

turn: also don't forward linklocal addresses

✓ e2f4094



franziskuskiefer reviewed on Mar 11, 2021

[View changes](#)

franziskuskiefer left a comment

Igtm if these are all the places this has to happen.
Do we have a way to test this?



arianvp suggested changes on Mar 11, 2021

[View changes](#)

modules/turn/turn.c Outdated

Show resolved

turn: block whole loopback range, also block broadcast

✓ 955064f

arianvp requested review from **arianvp** and **julialongtin** last year



✓ **arianvp** approved these changes on Mar 11, 2021

[View changes](#)

arianvp commented on Mar 11, 2021 • edited

Contributor

Using coturn's testing tools I'm checking if the relaying is being blocked. On the current build of restund indeed still relaying the addresses.:

```
$ nix run nixpkgs.coturn
$ turnutils_uclient -X 192.168.0.136 -u test -w secret -e 127.0.0.2 & turnutils_uclient -X 192.168.0.136 -u test -w secret -e 255.255.255.255 & turnutils_uclient -X 192.168.0.136 -u test -w secret -e 169.254.0.1
```

turn command on status interface shows 127.0.0.2, 255.255.255.255 and 169.254.0.1 being relayed

```
TURN relay=192.168.0.136 relay=? (err 5/0)
- 34295 UDP/192.168.0.136:34159/192.168.0.136:3478 - 192.168.0.136:38566 "test" 594s (drop 0/0)
  permissions: (169.254.0.1 295s relay 5/0)
  channels: (0x59c7 169.254.0.1:3481 595s)
- 37255 UDP/192.168.0.136:37119/192.168.0.136:3478 - 192.168.0.136:35496 "test" 655s (drop 0/0)
  permissions:
  channels:
- 37268 UDP/192.168.0.136:37132/192.168.0.136:3478 - 192.168.0.136:34725 "test" 594s (drop 0/0)
  permissions: (127.0.0.2 295s relay 5/0)
  channels: (0x6db7 127.0.0.2:3481 595s) (0x6fce 127.0.0.2:3480 595s)
- 37472 UDP/192.168.0.136:37336/192.168.0.136:3478 - 192.168.0.136:34724 "test" 771s (drop 0/0)
  permissions:
  channels:
- 42726 UDP/192.168.0.136:42590/192.168.0.136:3478 - 192.168.0.136:35114 "test" 156s (drop 0/0)
  permissions:
  channels:
- 43796 UDP/192.168.0.136:43660/192.168.0.136:3478 - 192.168.0.136:52394 "test" 594s (drop 0/0)
  permissions: (255.255.255.255 295s relay 0/0)
  channels: (0x701e 255.255.255.255:3481 595s)
- 47256 UDP/192.168.0.136:47120/192.168.0.136:3478 - 192.168.0.136:52854 "test" 594s (drop 0/0)
```

```
permissions: (127.0.0.2 295s relay 5/0)
channels: (0x6719 127.0.0.2:3481 595s)
- 47291 UDP/192.168.0.136:47155/192.168.0.136:3478 - 192.168.0.136:43029 "test" 594s (drop 0/0)
permissions: (169.254.0.1 295s relay 5/0)
channels: (0x45b8 169.254.0.1:3481 595s) (0x54fb 169.254.0.1:3480 595s)
- 52136 UDP/192.168.0.136:52000/192.168.0.136:3478 - 192.168.0.136:47978 "test" 631s (drop 0/0)
permissions:
channels:
- 52855 UDP/192.168.0.136:52719/192.168.0.136:3478 - 192.168.0.136:43028 "test" 771s (drop 0/0)
permissions:
channels:
- 54504 UDP/192.168.0.136:54368/192.168.0.136:3478 - 192.168.0.136:37080 "test" 771s (drop 0/0)
permissions:
channels:
- 55756 UDP/192.168.0.136:55620/192.168.0.136:3478 - 192.168.0.136:37081 "test" 594s (drop 0/0)
permissions: (255.255.255.255 295s relay 0/0)
channels: (0x77f2 255.255.255.255:3480 595s) (0x5455 255.255.255.255:3481 595s)
- 57837 UDP/192.168.0.136:57701/192.168.0.136:3478 - 192.168.0.136:46828 "test" 179s (drop 0/0)
permissions:
channels:
```

I will now make a new build and see if the issue is mitigated

 **arianvp** force-pushed the `block_local_any` branch 2 times, most recently from `53cffc7` to `c887de0` last year

[Compare](#)

 Add Dockerfile and github action ...

✓ c30f2f5

 **arianvp** force-pushed the `block_local_any` branch from `c887de0` to `c30f2f5` last year

[Compare](#)

 **arianvp** added 2 commits last year


 Also build the zrest and drain modules by default

✓ 20b0b9a

 Add entrypoint to dockerfile

✓ 1d4b671



 **arianvp** suggested changes on Mar 11, 2021

[View changes](#)

 **arianvp** left a comment

Contributor

@z-dule I tried to see if the issue at hand is fixed with this build; but I'm still able to successfully open a channel-bind on `127.0.0.1`.

```
192 Allocate Request UDP lifetime: 777 user: test with nonce realm: myrealm
164 Allocate Success Response XOR-RELAYED-ADDRESS: 192.168.0.136:41082 lifetime: 777 XOR-MAPPED-ADDRESS: 192.168.0.136:
168 Refresh Request lifetime: 777 user: test with nonce realm: myrealm
128 Refresh Success Response lifetime: 777
120 Channel-Bind Request ChannelNumber=0x47c9 XOR-PEER-ADDRESS: 127.0.0.1:3481 user: test with nonce realm: myrealm
120 Channel-Bind Success Response
180 Channel-Bind Request ChannelNumber=0x47c9 XOR-PEER-ADDRESS: 127.0.0.1:3481 user: test with nonce realm: myrealm
120 Channel-Bind Success Response
180 Channel-Bind Request ChannelNumber=0x7c89 XOR-PEER-ADDRESS: 127.0.0.1:3480 user: test with nonce realm: myrealm
120 Channel-Bind Success Response
180 Channel-Bind Request ChannelNumber=0x7c89 XOR-PEER-ADDRESS: 127.0.0.1:3480 user: test with nonce realm: myrealm
120 Channel-Bind Success Response
180 Channel-Bind Request ChannelNumber=0x5e50 XOR-PEER-ADDRESS: 127.0.0.1:3481 user: test with nonce realm: myrealm
120 Channel-Bind Success Response
168 Refresh Request lifetime: 600 user: test with nonce realm: myrealm
172 CreatePermission Request XOR-PEER-ADDRESS: 127.0.0.1:3480 user: test with nonce realm: myrealm
180 Channel-Bind Request ChannelNumber=0x7c89 XOR-PEER-ADDRESS: 127.0.0.1:3480 user: test with nonce realm: myrealm
128 Refresh Success Response lifetime: 600
120 CreatePermission Success Response
120 Channel-Bind Success Response
```

Maybe I'm missing something here. but it doesn't seem fixed.

arianvp commented on Mar 11, 2021 • edited

Contributor

Aaaah looking at the code where we add the check we're already past the channel-bind and at the "send data packets" part and we simply drop the packets on the floor. Is that correct?

But could we also add the check to

`restund/modules/turn/chan.c`
Line 232 in `edd4abd`

```
232 void chanbind_request(struct allocation *a1, struct restund_msgctx *ctx,
```


so that the channel-bind actually fails instead of accepting and silently dropping packets?

In short; also add the check to `request_handler`; not just `raw_handler` and `indication_handler`

would that make sense?

NOTE: This is me not knowing a lot about TURN so please tell me when I'm saying stupid things =)



 Disallow channel binding on blocked addresses

✓ deaef9c

 **arianvp** force-pushed the `block_local_any` branch 5 times, most recently from `384630e` to `3c2ec50` last year

[Compare](#)

 Add test to check relaying

✗ 22a5994

 **arianvp** force-pushed the `block_local_any` branch from `3c2ec50` to `22a5994` last year

[Compare](#)

Also still check for ::1 ...

✓ 87ca8fc

arianvp force-pushed the block_local_any branch from 29ea22c to 87ca8fc last year

Compare



✓ franziskuskiefer approved these changes on Mar 12, 2021

[View changes](#)

arianvp merged commit sc0ed84 into master on Mar 12, 2021
2 checks passed

View details

arianvp deleted the block_local_any branch last year

micmac1 mentioned this pull request on Dec 3, 2021

restund: status and open CVE openwrt/telephony#714

Closed

micmac1 added a commit to micmac1/telephony that referenced this pull request on Dec 6, 2021

restund: fix CVE-2021-21382 ...

dec6316

micmac1 added a commit to micmac1/telephony that referenced this pull request on Dec 6, 2021

restund: fix CVE-2021-21382 ...

4ca76cb

This was referenced on Dec 6, 2021

[21.02] restund: fix CVE-2021-21382 openwrt/telephony#716

Merged

[19.07] restund: fix CVE-2021-21382 openwrt/telephony#717

Merged

micmac1 added a commit to micmac1/telephony that referenced this pull request on Dec 8, 2021

restund: fix CVE-2021-21382 ...

612a753

micmac1 mentioned this pull request on Dec 8, 2021

restund: fix CVE-2021-21382 openwrt/telephony#720

Merged

Reviewers

arianvp



franziskuskiefer



julialongtin



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants

