Unsafe loopback forwarding interface

High **franziskuskiefer** published **GHSA-96j5-w9jq-pv2x** on Jun 11, 2021

Package

No package listed

Affected versions	Patched versions
<0.4.15	0.4.15

Description

Impact

The restund TURN server can be instructed to open a relay to the loopback address range. This allows you to reach any other service running on localhost which you might consider private. In the configuration that we ship (https://github.com/wireapp/ansible-restund/blob/master/templates/restund.conf.j2#L40-L43) the `status` interface of restund is enabled and is listening on `127.0.0.1` .The `status` interface allows users to issue administrative commands to `restund` like listing open relays or draining connections. It would be possible for an attacker to contact the status interface and issue administrative commands by setting `XOR-PEER-ADDRESS` to `127.0.0.1:{{restund_udp_status_port}}` when opening a TURN channel.

Mitigation

We now explicitly disallow relaying to loopback addresses, 'any' addresses, link local addresses, and the broadcast address.

See #7

Workarounds

- Disable the `status` module in your restund configuration. However there might still be other services running on `127.0.0.0/8` that you do not want to have exposed.
- The `turn` module can be disabled. Restund will still perform STUN and this might already be enough for initiating calls in your environments. TURN is only used as a last resort when other NAT traversal options do not work.

Further notes

One should also make sure that the TURN server is set up with firewall rules so that it cannot relay to other addresses that you don't want the TURN server to relay to. For example other services in the same VPC where the TURN server is running. Ideally TURN servers should be deployed in an isolated fashion where they can only reach what they need to reach to perform their task of assisting NAT-traversal.

Also see https://www.rtcsec.com/post/2021/01/details-about-cve-2020-26262-bypass-of-coturns-default-access-control-protection/#further-concerns-what-else

References

A more detailed analysis of the issue in coturn: https://www.rtcsec.com/post/2021/01/details-about-cve-2020-26262-bypass-of-coturns-default-access-control-protection/ and https://talosintelligence.com/vulnerability_reports/TALOS-2018-0732

For more information

This is the same issue that was recently fixed in coturn: GHSA-6g6j-r9rf-cm7p

Severity

High

CVE ID

CVE-2021-21382

Weaknesses

No CWEs