Talos Vulnerability Report

TALOS-2018-0732

coTURN TURN server unsafe loopback forwarding default configuration vulnerability

JANUARY 29, 2018

CVE NUMBER

CVE-2018-4058

Summary

An exploitable unsafe default configuration vulnerability exists in the TURN server functionality of coTURN prior to 4.5.0.9. By default, the TURN server allows relaying external traffic to the loopback interface of its own host. This can provide access to other private services running on that host, which can lead to further attacks. An attacker can set up a relay with a loopback address as the peer on an affected TURN server to trigger this vulnerability.

Tested Versions

coTURN 4.5.0.5

Product URLs

https://github.com/coturn/coturn

CVSSv3 Score

7.7 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N

CWE

CWE-250: Execution with Unnecessary Privileges

Details

coTURN is an open-source implementation of TURN and STUN servers that can be used as a general-purpose networking traffic TURN server. TURN servers are usually deployed in so-called “DMZ” zones — any server reachable by the internet — to provide firewall traversal solutions. Attackers who are able to take over such servers may be able to bypass firewalls and conduct further attacks.

According to Shodawn, thousands of coTURN servers are directly reachable on the internet.

The default options of affected coTURN servers allow TURN clients to set up peers being a loopback address. This setup forwards traffic from an external interface to a loopback interface of the server, and provides access to other services running on the loopback interface that would otherwise be private.

Mitigation

Run the coTURN server with the following option to disable loopback forwarding:

```
--no-loopback-peers                         Disallow peers on the loopback addresses (127.x.x.x and ::1)
```

Timeline

2017-09-04 - Vendor Disclosure
2019-01-28 - Vendor Patched
2019-01-29 - Public Release

CREDIT

Discovered by Nicolas Edet of Cisco.

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.