Product Notice #0483

SBC Security Configuration Update for Microsoft Teams Direct Routing

Customers using Microsoft Teams Direct Routing are advised to verify and update the security configuration of their SBC to prevent possible unauthorized calls

- A vulnerability was recently discovered in the default SBC security configuration allowing a potential attacker to place calls as a legitimate Teams user. This notice provides configuration instructions to mitigate and resolve this issue.
- The security configuration described in this notice should be applied to SBCs that are used for Microsoft Teams Direct Routing. There is no need to perform a software update for applying the recommendations, the changes are not service affecting.
- AudioCodes' SBC installation Wizard was updated according to this notice. To use the new wizard settings, update your SBC wizard to use template version 2.57 or above before using it for new Microsoft Teams Direct Routing installations.

Impact

- Without applying the recommended configuration update, an unauthenticated attacker could be able to send specially crafted SIP messages that pretend to originate from Microsoft and make unauthorized external calls; this may allow an attacker to make calls impersonating to be a legitimate user or to perform toll fraud.

Mitigation

- **Step 1 - Apply SBC Classification Rules that only allow Teams calls from official Microsoft Teams Servers**

  SBC Classification rule can be used to allow only specific SIP traffic to be accepted, acting as a SIP firewall. By adding Classification rules to the SBC configuration, the SBC will only allow SIP calls originating from the official Microsoft Teams SIP servers, these official Microsoft servers are resolved only to IP addresses from the following subnets: 52.112.0.0/14 and 52.120.0.0/14

Configure the SBC Classification table with the following classification rules:
A Classification rule classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a "source" IP Group. The source IP Group is the SIP entity that sends the SIP dialog request, in the following configuration, used also in our Microsoft Direct Routing configuration guide , this IP Group is simply called "Teams". It is also assumed that the Message Condition "Teams-Contact" was defined according to our configuration guide.

To configure a Classification rule:

1. Open the Classification table (Setup menu > Signaling & Media tab > SBC folder > Classification Table).

2. Configure Classification rules as shown in the table below (use the FQDN name of the SBC in the Enterprise Office 365 tenant as Destination Host):

Index	Name	Source SIP Interface	Source IP Address	Destination Host	Message Condition	Action Type	Source IP Group
0	Teams_52_112 (arbitrary name)	Teams	52.112.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
1	Teams_52_113 (arbitrary name)	Teams	52.113.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
2	Teams_52_114 (arbitrary name)	Teams	52.114.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
3	Teams_52_115 (arbitrary name)	Teams	52.115.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
4	Teams_52_120 (arbitrary name)	Teams	52.120.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
5	Teams_52_121 (arbitrary name)	Teams	52.121.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
6	Teams_52_122 (arbitrary name)	Teams	52.122.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams
7	Teams_52_123 (arbitrary name)	Teams	52.123.*.*	sbc.ACeducation.info (example)	Teams-Contact	Allow	Teams

3.click **Apply**

These settings will only allow incoming calls from the Microsoft Teams SIP servers to be identified as coming from Teams, which will prevent exploiting the vulnerability.

- **Step 2 - Configure SBC Firewall rules**

  Although the previous step provides sufficient mitigation, this extra step can be used as an additional security measure by adding traffic filtering rules (access list) for incoming traffic. Using these firewall rules, the SBC will only allow TCP traffic originating from the official Microsoft Teams SIP subnets.
  Follow the steps to configure SBC firewall settings as described in our Microsoft Direct Routing configuration guide, if not already done so previously.

Actions taken by AudioCodes

- **Update of the SBC configuration wizard**: The SBC configuration wizard Teams configuration template version 2.57 was updated according to the recommendations in this notice.
- **Update of the Microsoft Teams Configuration guide** : The Microsoft Direct Routing configuration guide was updated according to the recommendations in this notice.
- In case that Microsoft adds new subnets to its Teams service, AudioCodes will notify accordingly.

Affected Products

- Software and hardware-based SBCs used for Microsoft Teams Direct Routing.

If you have any questions, contact us at
https://www.audiocodes.com/corporate/offices-worldwide
AudioCodes Ltd. | 1 Hayarden Street | Airport City | Lod | Israel | +972-3-976-4000