ASSERTION®

ASSERTION Security Assessment Report

06, February 2021 (GMT)

This report was auto-generated by ASSERTION ® Audit

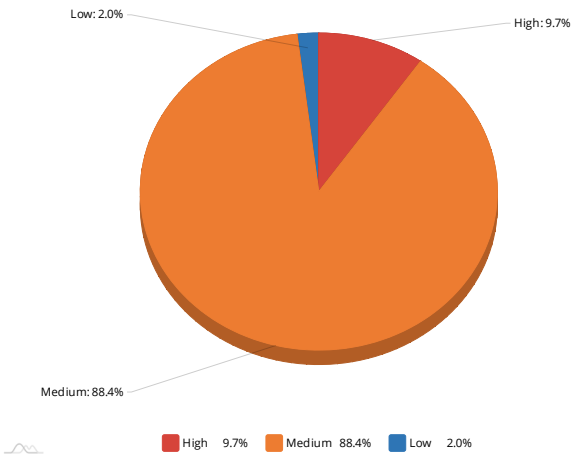
Executive Summary

Your SBC configuration does not adhere to most of the security guidelines, while security risks can be observed in the areas of ***Management Access Restriction, Single Source DoS, Phone DoS DDoS, Call Walking DDoS, Session Security, Advance Session Security, Remote Worker Admission, End to End Media Encryption and Trunk Gateway Admission***.

53	728	37
Breaches	Attacks	Security Configuration

7 security checks were suppressed because of insufficient data.

Total security issues



Any **HIGH** and **MEDIUM** severity issues should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other issues to enable further attacks.

Introduction

Application details

Application Vendor	Avaya
Application (Integration) Family	SBC
Application Name	Avaya Session Border Controller
SBC Mode	Remote Worker & Trunk Gateway
SBC Deployment Type	Non-HA
Hostname	172.16.2.5
Scan Date	February 6, 2021
Scanned By	satyam@assertion.cloud

Approach

We connect to the EMS IP address and collect the configuration data of the desired SBC. We collect the audit and trace log for 30 days.

We analyse the log for patterns of security incidents, abnormal traffic and system alarms. We check the configuration against Assertion's high security standard for SBCs. Assertion's standard for SBC security goes over and beyond Avaya's SBC security guidelines.

Data Scanned

Configuration
48 item(s)

Logs
13.74 million logs

CDR / call logs
Not applicable

Audio
Not applicable

Screen & Video
Not applicable

Text
Not applicable

Breach details

Check : Breach Detection by Successful Registration from Unknown User Agent Threat level : High					
Instance	**Target**	**Attack Source**	**Attack Signature**	**Date & Time**	**Evidence**
2	3221	42.96.64.120	Compromised extension - suspicious user agent	12-01-2020 07:06:07	tracesbc_sip_1606789915_1606793505_1.gz
2	3222	42.96.6.120	Compromised extension - suspicious user agent	12-01-2020 07:06:41	tracesbc_sip_1606789914_1606793505_1.gz
1	9283	40.129.144.136	Compromised extension - suspicious user agent	10-29-2020 11:12:48	tracesbc_sip_1603952854_1603956435_1.gz
17	9283	40.129.144.110	Compromised extension - suspicious user agent	10-30-2020 01:55:19	tracesbc_sip_1603978055_1603981644_1.gz, tracesbc_sip_1603981656_1603985254_1.gz, tracesbc_sip_1603988856_1603992455_1.gz, tracesbc_sip_1603992456_1603996050_1.gz, tracesbc_sip_1603999656_1604003227_1.gz, tracesbc_sip_1604003257_1604006840_1.gz, tracesbc_sip_1603985256_1603988849_1.gz, tracesbc_sip_1603996056_1603999656_1.gz, tracesbc_sip_1604006857_1604010437_1.gz
1	9283	40.129.144.239	Compromised extension - suspicious user agent	10-29-2020 07:11:33	tracesbc_sip_1603938423_1603942003_1.gz
11	9283	40.129.144.129	Compromised extension - suspicious user agent	10-29-2020 17:21:47	tracesbc_sip_1603956454_1603960040_1.gz, tracesbc_sip_1603960055_1603963648_1.gz, tracesbc_sip_1603963655_1603967225_1.gz, tracesbc_sip_1603970855_1603974436_1.gz, tracesbc_sip_1603974455_1603978025_1.gz, tracesbc_sip_1603967255_1603970850_1.gz
10	9283	40.129.144.110	Compromised extension - suspicious user agent	10-29-2020 10:51:49	tracesbc_sip_1603945624_1603949224_1.gz, tracesbc_sip_1603938423_1603942003_1.gz, tracesbc_sip_1603942024_1603945621_1.gz, tracesbc_sip_1603949254_1603952833_1.gz, tracesbc_sip_1603952854_1603956435_1.gz
1	9283	40.129.144.13	Compromised extension - suspicious user agent	10-29-2020 10:51:51	tracesbc_sip_1603952854_1603956435_1.gz
1	9283	40.129.144.96	Compromised extension - suspicious user agent	10-31-2020 21:46:20	tracesbc_sip_1604165265_1604168842_1.gz

3	9283	40.129.3.119	Compromised extension - suspicious user agent	10-29-2020 11:13:04	tracesbc_sip_1603938423_1603942003_1.gz, tracesbc_sip_1603952854_1603956435_1.gz

Metadata:

Risk category: Remote Worker Security	Security Policy: Suspicious Endpoint Type Registrations
Impact / Fallout: Unauthorized access to enterprise service	Violation : Restrict registration from unknown endpoint types

Description : Breach detection by successful registration from unknown User Agent

Recommendation :

1. We have observed successful registration from endpoint type's which is not familiar in your setup. Following endpoint type were observed:
   - eyeBeam communicator 3.14 : 45
   - Avaya Phone : 4
2. Change the user agent filter on all the subscriber flow to ensure eyeBeam communicator 3.14 and Avaya Phone are blocked.

Check : Breach detection by Registration from a suspicious subnet
Threat level : High

Instance	Target	Attack Source	Attack Signature	Date & Time	Evidence
2	4521	39.109.98.103	Compromised endpoint - suspicious registration	12-01-2020 07:06:07	tracesbc_sip_1606789918_1606793505_1.gz
2	4522	39.109.98.103	Compromised endpoint - suspicious registration	12-01-2020 07:06:41	tracesbc_sip_1606789918_1606793505_1.gz

Metadata:

Risk category: Remote Worker Security	Security Policy: Registrations from Known Suspicious Subnets
Impact / Fallout: User impersonation leading to enterprise fraud	Violation : Restrict registration from unknown network

Description : Detect Breach by successful registration from suspected IP address

Recommendation :

1. We have observed successful REGISTER from suspected IP address for the extension mentioned in the Target.
2. It is highly recommended to blacklist suspected IP addresses, enable user agent filtering and enable mutual authentication on the subscriber flow.

Threat Observed

Check : Single Source Brute Force Attempt **Threat level : High**					
Instance	**Target**	**Attack Source**	**Attack Signature**	**Date & Time**	**Evidence**
2	8423 (16)	39.109.70.36	Remote worker brute force	12-01-2020 10:06:09	tracesbc_sip_1606789916_1606793505_1.gz
Metadata:					
Risk category: Remote Worker Security			Security Policy: Brute Force Registration Attacks		
Impact / Fallout: Remote worked extension take over			Violation : Remote worker login attempt restrictions		
Description : Brute force attempts on single extension					
Recommendation : 1. We have observed brute force attempts on the specified extensions 2. If this is not a legitimate SourceIP and found targeting multiple extensions, blacklist the IP address. Consider enable mutual authentication if the extension belongs to a high value employee.					

Check : Detect Impossible Travel to an Atypical Location
Threat level : Medium

Instance	Target	Attack Source	Attack Signature	Date & Time	Evidence
4	9656	PrevLoc: OM|Muscat Loc: FR|Hauts-de-France	Impossible travel to an atypical location	11-12-2020 20:22:13	tracesbc_sip_1605194927_1605198514_1.gz
4	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Île-de-France	Impossible travel to an atypical location	12-05-2020 13:29:32	tracesbc_sip_1607157194_1607160792_1.gz
3	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Grand Est	Impossible travel to an atypical location	12-01-2020 09:35:59	tracesbc_sip_1606800714_1606804313_1.gz
2	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Grand Est	Impossible travel to an atypical location	12-05-2020 09:20:16	tracesbc_sip_1607142765_1607146365_1.gz
4	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Grand Est	Impossible travel to an atypical location	12-05-2020 11:32:42	tracesbc_sip_1607149977_1607153566_1.gz
5	9656	PrevLoc: NL|North Holland Loc: OM|Muscat	Impossible travel to an atypical location	11-08-2020 10:45:33	tracesbc_sip_1604816904_1604820481_1.gz
4	9656	PrevLoc: FR|Île-de-France Loc: OM|Al Batinah North	Impossible travel to an atypical location	11-19-2020 09:35:39	tracesbc_sip_1605763821_1605767410_1.gz
2	9656	PrevLoc: OM|Muscat Loc: NL|South Holland	Impossible travel to an atypical location	11-06-2020 20:03:15	tracesbc_sip_1604676496_1604680079_1.gz
3	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Muscat	Impossible travel to an atypical location	12-05-2020 22:57:49	tracesbc_sip_1607193198_1607196768_1.gz
2	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Muscat	Impossible travel to an atypical location	12-02-2020 09:02:21	tracesbc_sip_1606883549_1606887145_1.gz
4	9656	PrevLoc: DE|Saarland Loc: OM|Muscat	Impossible travel to an atypical location	11-27-2020 06:26:13	tracesbc_sip_1606440663_1606444244_1.gz
4	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Muscat	Impossible travel to an atypical location	11-12-2020 20:25:56	tracesbc_sip_1605194927_1605198514_1.gz
4	9656	PrevLoc: DE|Hesse Loc: OM|Muscat	Impossible travel to an atypical location	11-12-2020 20:14:30	tracesbc_sip_1605194927_1605198514_1.gz

3	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Muscat	Impossible travel to an atypical location	11-09-2020 14:53:58	tracesbc_sip_1604917710_1604921309_1.gz
4	9656	PrevLoc: GB|England Loc: OM|Muscat	Impossible travel to an atypical location	11-07-2020 06:43:20	tracesbc_sip_1604716098_1604719686_1.gz
2	9656	PrevLoc: NL|South Holland Loc: OM|Muscat	Impossible travel to an atypical location	11-06-2020 20:42:47	tracesbc_sip_1604680096_1604683683_1.gz
3	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Muscat	Impossible travel to an atypical location	11-12-2020 16:28:48	tracesbc_sip_1605184126_1605187724_1.gz
4	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Muscat	Impossible travel to an atypical location	11-08-2020 18:53:29	tracesbc_sip_1604845706_1604849288_1.gz
2	9656	PrevLoc: FR|Grand Est Loc: OM|Ad Dakhiliyah	Impossible travel to an atypical location	12-01-2020 09:39:40	tracesbc_sip_1606800714_1606804313_1.gz
4	9656	PrevLoc: DE|Hesse Loc: OM|Muscat	Impossible travel to an atypical location	11-18-2020 08:05:14	tracesbc_sip_1605670186_1605673762_1.gz
2	9656	PrevLoc: DE|Hesse Loc: OM|Muscat	Impossible travel to an atypical location	11-30-2020 21:41:42	tracesbc_sip_1606757512_1606761097_1.gz
5	9656	PrevLoc: FR|Île-de-France Loc: OM|Ad Dakhiliyah	Impossible travel to an atypical location	12-05-2020 13:48:56	tracesbc_sip_1607160796_1607164382_1.gz
2	9656	PrevLoc: FR|Grand Est Loc: OM|Ad Dakhiliyah	Impossible travel to an atypical location	12-05-2020 09:26:22	tracesbc_sip_1607142765_1607146365_1.gz
5	9656	PrevLoc: FR|Grand Est Loc: OM|Ad Dakhiliyah	Impossible travel to an atypical location	12-05-2020 11:43:28	tracesbc_sip_1607153591_1607157183_1.gz
6	9656	PrevLoc: FR|Île-de-France Loc: OM|Ad Dakhiliyah	Impossible travel to an atypical location	12-05-2020 10:36:57	tracesbc_sip_1607149977_1607153566_1.gz
2	9656	PrevLoc: FR|Hauts-de-France Loc: OM|Ad Dakhiliyah	Impossible travel to an atypical location	12-05-2020 10:36:39	tracesbc_sip_1607149977_1607153566_1.gz
4	9656	PrevLoc: FR|Île-de-France Loc: OM|Al Batinah North	Impossible travel to an atypical location	12-04-2020 21:24:36	tracesbc_sip_1607099562_1607103158_1.gz
4	9656	PrevLoc: OM|Muscat Loc: NL|North Holland	Impossible travel to an atypical location	11-08-2020 10:30:10	tracesbc_sip_1604816904_1604820481_1.gz

4	9656	PrevLoc: OM|Al Batinah North Loc: FR|Île-de-France	Impossible travel to an atypical location	11-19-2020 09:32:14	tracesbc_sip_1605763821_1605767410_1.gz
2	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Île-de-France	Impossible travel to an atypical location	12-05-2020 10:36:53	tracesbc_sip_1607149977_1607153566_1.gz
4	9656	PrevLoc: OM|Al Batinah North Loc: FR|Île-de-France	Impossible travel to an atypical location	12-04-2020 20:28:19	tracesbc_sip_1607095962_1607099552_1.gz
4	9656	PrevLoc: OM|Muscat Loc: DE|Hesse	Impossible travel to an atypical location	11-12-2020 20:11:47	tracesbc_sip_1605194927_1605198514_1.gz
4	9656	PrevLoc: OM|Muscat Loc: GB|England	Impossible travel to an atypical location	11-07-2020 06:26:39	tracesbc_sip_1604712498_1604716090_1.gz
4	9656	PrevLoc: OM|Muscat Loc: FR|Hauts-de-France	Impossible travel to an atypical location	11-09-2020 14:47:20	tracesbc_sip_1604917710_1604921309_1.gz
4	9656	PrevLoc: OM|Muscat Loc: FR|Hauts-de-France	Impossible travel to an atypical location	11-08-2020 18:32:26	tracesbc_sip_1604845706_1604849288_1.gz
2	9656	PrevLoc: OM|Muscat Loc: FR|Hauts-de-France	Impossible travel to an atypical location	12-02-2020 08:57:19	tracesbc_sip_1606883549_1606887145_1.gz
2	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Hauts-de-France	Impossible travel to an atypical location	12-05-2020 09:53:54	tracesbc_sip_1607146377_1607149977_1.gz
2	9656	PrevLoc: OM|Muscat Loc: DE|Saarland	Impossible travel to an atypical location	11-27-2020 06:24:05	tracesbc_sip_1606440663_1606444244_1.gz
3	9656	PrevLoc: OM|Ad Dakhiliyah Loc: FR|Hauts-de-France	Impossible travel to an atypical location	12-05-2020 22:25:05	tracesbc_sip_1607189598_1607193182_1.gz
4	9656	PrevLoc: OM|Muscat Loc: DE|Hesse	Impossible travel to an atypical location	11-30-2020 21:27:55	tracesbc_sip_1606753912_1606757502_1.gz
4	9656	PrevLoc: OM|Northeastern Governorate Loc: FR|Hauts-de-France	Impossible travel to an atypical location	11-12-2020 16:22:43	tracesbc_sip_1605180526_1605184118_1.gz
4	9656	PrevLoc: OM|Muscat Loc: DE|Hesse	Impossible travel to an atypical location	11-18-2020 07:54:53	tracesbc_sip_1605670186_1605673762_1.gz

2	9663	PrevLoc: OM|Al Batinah North Loc: US|New Jersey	Impossible travel to an atypical location	11-27-2020 23:49:07	tracesbc_sip_1606505467_1606509050_1.gz
2	9663	PrevLoc: OM|Muscat Loc: US|New Jersey	Impossible travel to an atypical location	11-28-2020 14:36:35	tracesbc_sip_1606559470_1606563056_1.gz
2	9663	PrevLoc: US|New Jersey Loc: OM|Muscat	Impossible travel to an atypical location	11-28-2020 14:58:25	tracesbc_sip_1606559470_1606563056_1.gz
2	9663	PrevLoc: US|New Jersey Loc: OM|Al Batinah North	Impossible travel to an atypical location	11-28-2020 00:21:37	tracesbc_sip_1606505467_1606509050_1.gz
2	9683	PrevLoc: OM|Al Batinah North Loc: NL|North Holland	Impossible travel to an atypical location	11-28-2020 20:14:31	tracesbc_sip_1606577480_1606581078_1.gz
4	9689	PrevLoc: IN|Tamil Nadu Loc: NL|North Holland	Impossible travel to an atypical location	12-02-2020 02:45:59	tracesbc_sip_1606861948_1606865546_1.gz

Metadata:

Risk category: Remote Worker Security	Security Policy: Impossible Travel to an Atypical Location
Impact / Fallout: User impersonation leading to enterprise fraud	Violation : Impossible activity from geographically distinct locations

Description : Detect Impossible Time Travel attack attempt on a single endpoint

Recommendation :

1. We have observed registration attempts on specified targets from location which are impossible for a user to travel in a short duration.
2. If these are not legitimate attempts we highly recommend to change the credentials and force un-register all the registered extensions.

Check : Detect call attempts to an unfamiliar location
Threat level : Medium

Instance	Target	Attack Source	Attack Signature	Date & Time	Evidence
1	+36345856	6579	Toll fraud - unfamiliar number	12-03-2020 20:05:36	tracesbc_sip_1607009557_1607013156_1.gz
4	+916394329	2356	Toll fraud - unfamiliar number	11-10-2020 10:07:19	tracesbc_sip_1604204867_1604208452_1.gz, tracesbc_sip_1604986114_1604989712_1.gz
1	+9176303202	2356	Toll fraud - unfamiliar number	11-01-2020 09:22:11	tracesbc_sip_1604204867_1604208452_1.gz
1	+971253600	3256	Toll fraud - unfamiliar number	11-04-2020 16:11:09	tracesbc_sip_1604489284_1604492877_1.gz
1	+97146655	4856	Toll fraud - unfamiliar number	11-04-2020 16:24:28	tracesbc_sip_1604489284_1604492877_1.gz
2	00919185784	4856	Toll fraud - unfamiliar number	11-10-2020 10:08:20	tracesbc_sip_1604986114_1604989712_1.gz
1	009989172308	4856	Toll fraud - unfamiliar number	11-01-2020 09:09:20	tracesbc_sip_1604204867_1604208452_1.gz
4	008552588036	3489	Toll fraud - unfamiliar number	11-10-2020 13:06:22	tracesbc_sip_1603898732_1603902323_1.gz, tracesbc_sip_1604579290_1604582862_1.gz, tracesbc_sip_1604834905_1604838497_1.gz, tracesbc_sip_1604996915_1605000506_1.gz
1	009101026795	3456	Toll fraud - unfamiliar number	11-06-2020 19:39:12	tracesbc_sip_1604676496_1604680079_1.gz
27	001564557351	3489	Toll fraud - unfamiliar number	11-16-2020 16:32:31	tracesbc_sip_1604986114_1604989712_1.gz, tracesbc_sip_1605169725_1605173323_1.gz, tracesbc_sip_1605166125_1605169721_1.gz, tracesbc_sip_1604471283_1604474880_1.gz, tracesbc_sip_1604482084_1604485669_1.gz, tracesbc_sip_1605173326_1605176923_1.gz, tracesbc_sip_1605529777_1605533375_1.gz, tracesbc_sip_1604485684_1604489274_1.gz, tracesbc_sip_1605108522_1605112111_1.gz, tracesbc_sip_1605526177_1605529756_1.gz
2	1050	3489	Toll fraud - unfamiliar number	11-12-2020 16:01:52	tracesbc_sip_1605180526_1605184118_1.gz
2	1070	3489	Toll fraud - unfamiliar number	11-12-2020 16:40:37	tracesbc_sip_1605184126_1605187724_1.gz
1	223844173	2357	Toll fraud - unfamiliar number	11-23-2020 11:26:14	tracesbc_sip_1606113042_1606116633_1.gz

2	243415199	3489	Toll fraud - unfamiliar number	11-12-2020 16:01:11	tracesbc_sip_1605180526_1605184118_1.gz
2	5632	8769	Toll fraud - unfamiliar number	10-28-2020 20:36:13	tracesbc_sip_1603898732_1603902323_1.gz, tracesbc_sip_1603902332_1603905932_1.gz
1	9999	3489	Toll fraud - unfamiliar number	11-12-2020 16:02:13	tracesbc_sip_1605180526_1605184118_1.gz
2	2342	3489	Toll fraud - unfamiliar number	11-12-2020 16:44:57	tracesbc_sip_1605184126_1605187724_1.gz
1	62399	3489	Toll fraud - unfamiliar number	11-12-2020 15:59:51	tracesbc_sip_1605180526_1605184118_1.gz
2	6302	3489	Toll fraud - unfamiliar number	11-12-2020 16:42:13	tracesbc_sip_1605184126_1605187724_1.gz
1	7252341016	3456	Toll fraud - unfamiliar number	11-04-2020 17:06:49	tracesbc_sip_1604492884_1604496478_1.gz
1	23456001	3456	Toll fraud - unfamiliar number	11-16-2020 12:17:02	tracesbc_sip_1605511776_1605515362_1.gz
4	902341940	3456	Toll fraud - unfamiliar number	11-16-2020 16:46:39	tracesbc_sip_1605529777_1605533375_1.gz
1	91171188	83463	Toll fraud - unfamiliar number	11-07-2020 11:14:47	tracesbc_sip_1604730499_1604734098_1.gz
1	92234100	3456	Toll fraud - unfamiliar number	11-04-2020 17:04:42	tracesbc_sip_1604492884_1604496478_1.gz
1	9245611	3456	Toll fraud - unfamiliar number	11-08-2020 19:40:23	tracesbc_sip_1604849306_1604852903_1.gz
1	94156763	3456	Toll fraud - unfamiliar number	12-03-2020 15:42:07	tracesbc_sip_1606995156_1606998752_1.gz
1	92332	3456	Toll fraud - unfamiliar number	11-20-2020 15:13:14	tracesbc_sip_1605868227_1605871803_1.gz
1	9456456494	3456	Toll fraud - unfamiliar number	11-08-2020 19:41:15	tracesbc_sip_1604849306_1604852903_1.gz
1	66793450	3456	Toll fraud - unfamiliar number	11-20-2020 15:13:03	tracesbc_sip_1605868227_1605871803_1.gz
1	212358966	3463	Toll fraud - unfamiliar number	11-22-2020 12:45:07	tracesbc_sip_1606033838_1606037416_1.gz

1	21344224	3456	Toll fraud - unfamiliar number	12-06-2020 13:24:57	tracesbc_sip_1607243601_1607247199_1.gz
1	21346493	3456	Toll fraud - unfamiliar number	11-22-2020 08:30:44	tracesbc_sip_1606019436_1606023015_1.gz
1	123414913	3457	Toll fraud - unfamiliar number	11-23-2020 10:40:08	tracesbc_sip_1606113042_1606116633_1.gz
1	45672882	3456	Toll fraud - unfamiliar number	11-26-2020 15:56:58	tracesbc_sip_1606390259_1606393859_1.gz

Metadata:

Risk category: Toll Fraud	Security Policy: Toll Fraud Attempt Spikes
Impact / Fallout: Illegitimate outbound calls made outside business interest	Violation : Restrict outside usual business location calling

Description : Potential Toll Fraud - Outbound call to unfamiliar number range

Recommendation :

1. We have observed that calls are made to un-familiar number. These may be the calls made to outside business numbers.
2. If these dialled outbound numbers are no legitimate block them on the session manager routing or communication manager

Check : Detect unwanted traffic Threat level : Low					
Instance	**Target**	**Attack Source**	**Attack Signature**	**Date & Time**	**Evidence**
0 / 7616	Remote Worker Func.	39.109.98.43	White noise visibility	12-01-2020 00:00:00	NA
4 / 16	Remote Worker Func.	39.109.98.36	White noise visibility	12-01-2020 00:00:00	NA
3 / 14	Trunk Gateway Func.	39.109.98.36	White noise visibility	12-01-2020 00:00:00	NA
Metadata:					
Risk category: DoS, DDoS and Cyber attacks			Security Policy: Whitenoise Detection		
Impact / Fallout: Disruption of service due to high unwanted traffic on the SBC			Violation : Block recon attempts for chained attack		
Description : Legit vs unwanted traffic					
Recommendation : 1. We have observed unwanted traffic from the IP address mentioned. 2. You may want to black list the IP address where all the messages are rejected.					

Security Configuration Holes

Check : Single Source DoS Feature Status Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	DoS/DDoS Protection	Single source DoS protection is disabled	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient DoS/DDoS Restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the single source DoS feature is enabled				
Recommendation : 1. We have observed that the value of Single Source DoS is not appropriately set. 2. Your current configuration is Single Source DoS Protection Enabled = false. 3. We recommend to change the values as following: ○ Single Source DoS Protection should be enabled 4. Configuration can be found at following navigate path "Network & Flows"=>"Advanced Options"=>"Feature Control"=>"Single Source DoS Protection" of the EMS web portal.				

Check : Single Source DoS Handling Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	DoS/DDoS Protection	Single source DoS parameter misconfiguration.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient DoS/DDoS Restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the single source DoS is configured appropriately on the system				
Recommendation : 1. We have observed that the value of Single Source DoS parameteres are not appropriately configured. 2. Your current configuration is Single Source DoS Protection is Disabled. 3. We recommend to change the values as following: ○ SIP Method = All ○ Threshold = 300 ○ Action in Block 4. Configuration can be found at following navigate path "System Parameters"=>"Dos / DDoS"=>"Single Source DoS" of the EMS web portal.				

Check : Phone DoS/DDoS Feature Status Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	DoS/DDoS Protection	Phone DoS/DDoS protection is disabled.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient DoS/DDoS Restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the phone DoS feature is enabled				

Recommendation :

1. We have observed that the value of Single Source DoS is not appropriately set.
2. Your current configuration is Phone DoS/DDoS Protection Enabled = false.
3. We recommend to change the values as following:
    - Phone DoS/DDoS Protection should be enabled.
4. Configuration can be found at following navigate path "Network & Flows"=>"Advanced Options"=>"Feature Control"=>"Phone DoS / DDoS Protection" of the EMS web portal.

Check : Phone DoS/DDoS Handling Check

Instance	Target	Findings	Date & Time	Evidence
1	DoS/DDoS Protection	Phone DoS/DDoS parameter misconfiguration.	02-01-2021 11:40:17	NA

Metadata

Risk category : DoS, DDoS and Cyber attacks	Security Policy: Insufficient DoS/DDoS Restrictions
Impact / Fallout : NA	Violation: NA

Description : Verify the phone DoS is configured appropriately on the system

Recommendation :

1. We have observed that the value of Phone DoS / DDoS parameteres are not appropriately configured.
2. Your current configuration is Phone DDoS Protection is Disabled.
3. We recommend to change the values as following:
    - SIP Service = Ignore
    - SIP Method = All
    - Threshold = 200
    - Action in Block
4. Configuration can be found at following navigate path "System Parameters"=>"Dos / DDoS"=>"Phone DoS / DDoS" of the EMS web portal.

Check : Admission Control Restricted User Agent Check

Instance	Target	Findings	Date & Time	Evidence
1	Remote Worker	Insure User Agent restrictions.	02-01-2021 11:40:17	NA

Metadata

Risk category : Remote Worker Security	Security Policy: Insufficient Device and Extension Restrictions
Impact / Fallout : NA	Violation: NA

Description : Verify the admission control value of User Agent is configured appropriately on the system

Recommendation :

1. We have observed that user agent restrictions on the subscriber flow are not appropriately configured.
2. Your current configuration is
    - User Agent = *
3. We recommend to change the values to restrict only following user agents list
    - Avaya Communicator Android/3.12.0
    - Avaya Communicator Android/3.13.0
    - Avaya CM/R017x.01.0.532.0 AVAYA-SM-7.1.3.5.713507
    - Avaya Communicator Android/3.14.0
    - Avaya Communicator for iPhone/3.13.0
    - Avaya Communicator for iPhone/3.14.0
    - Avaya Communicator/3.0
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>"User Agent"

Check : Remote Worker Media Security Check

Instance	Target	Findings	Date & Time	Evidence
1	Remote Worker	Insecure media encryption.	02-01-2021 11:40:17	NA
Metadata				
Risk category : Data Leaks			Security Policy: Insecure Media Configurations	
Impact / Fallout : NA			Violation: NA	
Description : Verify the media encryption related parameters are configured appropriately on the system				

Recommendation :

1. We have observed the media is not encrypted to prevent data leaks.
2. Your current cofiguration is
   - Audio RTP Encryption = RTP
   - Audio Encrypted RTCP = undefined
   - Video RTP Encryption = RTP
   - Video Encrypted RTCP = undefined
3. It is highly recommended that the Encryption type in the MediaRules of the SBC is selected as SRTP. Ensure that all the preferred formats do not have RTP or NONE. Select a secured MediaRule on your subscriber flow.
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>"User Agent"

Check : Remote Worker Signaling Interface Transport Check

Instance	Target	Findings	Date & Time	Evidence
1	Remote Worker	Insecured signaling interface.	02-01-2021 11:40:17	NA
Metadata				
Risk category : Data Leaks			Security Policy: Insecure Signaling Configurations	
Impact / Fallout : NA			Violation: NA	
Description : Verify the signaling interface transport is TLS				

Recommendation :

1. We have observed that insecured signaling interface is selected.
2. Your current cofiguration is
   - TLS Port = NaN
   - TCP Port = 5060
   - UDP Port = 5060
3. It is highly recommended that you select a secured signaling interface
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>

Check : Remote Worker TLS Security Check - Client

Instance	Target	Findings	Date & Time	Evidence
1	Remote Worker	Insecured TLS Client security.	02-01-2021 11:40:17	NA
Metadata				
Risk category : Data Leaks			Security Policy: Prevent information leaks through strong ciphers	
Impact / Fallout : NA			Violation: NA	
Description : Verify the TLS client profile parameters are configured appropriately on the system				

Recommendation :

1. We have observed that the TLS Profile {"key":"NA"} is not securely cofigured.
2. Your current cofiguration is
   - TLS Server Profile = None
3. We recommend to change the configuration as follows
   - TLS Version in TLS 1.2
   - TLS Ciphers in Ignore
   - Peer Verification = Ignore
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>

Check : Default User Status Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
2	Default local user	Default user is active	02-01-2021 11:40:17	NA
Metadata				
Risk category : Alignment with Standards			Security Policy: Default account restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the status of the local user is as expected.				
Recommendation : 1. We have observed that default user ucsec is configured on the system with permissions Role = System Administrator , Type = Local , Status = Normal to access the management console. 2. Ensure that the default is disabled and an equivalent account is created.				

Check : Call Walking Feature Status Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	DoS/DDoS Protection	Call walking protection is disabled.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient DoS/DDoS Restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the call walking feature is enabled				
Recommendation : 1. We have observed that the value of Call walking DoS is not appropriately set. 2. Your current configuration is Call Walking Enabled = false. 3. We recommend to change the values as following: - Call Walking Protection should be enabled 4. Configuration can be found at following navigate path "Network & Flows"=>"Advanced Options"=>"Feature Control"=>"Call Walking Protection" of the EMS web portal.				

Check :Call Walking Handling Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	DoS/DDoS Protection	Call Walking parameter misconfiguration.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient DoS/DDoS Restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the stealth DoS feature is enabled				

Recommendation :
1. We have observed that the value of Call Walking parameteres are not appropriately configured.
2. Your current configuration is Stealth Enabled = false.
3. We recommend to change the values as following as per the OEM security guide:
    - Stealth Enabled = True
4. Configuration can be found at following navigate path "System Parameters"=>"Dos / DDoS"=>"Call Walking" of the EMS web portal.

Check : Call Walking Handling Check

Instance	Target	Findings	Date & Time	Evidence
1	DoS/DDoS Protection	Call Walking parameter misconfiguration.	02-01-2021 11:40:17	NA

Metadata

Risk category : DoS, DDoS and Cyber attacks	Security Policy: Insufficient DoS/DDoS Restrictions
Impact / Fallout : NA	Violation: NA

Description : Verify the stealth DoS is configured appropriately on the system

Recommendation :
1. We have observed that the value of Call Walking parameteres are not appropriately configured.
2. Your current configuration is Stealth Ddos is not configured.
3. We recommend to change the values as following as per the OEM security guide:
    - Approved User parameters
4. Configuration can be found at following navigate path "System Parameters"=>"Dos / DDoS"=>"Call Walking" of the EMS web portal.

Check : Remote Worker Other Security Parameters Check

Instance	Target	Findings	Date & Time	Evidence
1	Remote Worker	Other security parameters.	02-01-2021 11:40:17	NA

Metadata

Risk category : Data Leaks	Security Policy: Insecure Signaling Configurations
Impact / Fallout : NA	Violation: NA

Description : Verify the other security parameters are configured appropriately on the system

Recommendation :
1. We have observed that one of the additional security parameters have security concerns.
2. Your current cofiguration is
    - Methods Allowed Before Registration =
    - Routing Transport = Auto-Detect,UDP
    - Enable Natting = true
    - CDR Support = Off
3. We recommend to change the configuration as follows
    - Methods Allowed Before Registration in ASSERTION.BLANK
    - Routing Transport in Ignore
    - Enable Natting = True
    - CDR Support in Radius,CDR_Adjunct
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>

Check : Remote Worker TLS Security Check - Server

Instance	Target	Findings	Date & Time	Evidence
1	Remote Worker	Insecured TLS Client security.	02-01-2021 11:40:17	NA

Metadata

Risk category : Data Leaks	Security Policy: Prevent information leaks through strong ciphers
Impact / Fallout : NA	Violation: NA

Description : Verify the TLS server profile parameters are configured appropriately on the system

Recommendation :

1. We have observed that the TLS Profile {"key":"NA"} is not securely cofigured.
2. Your current cofiguration is
   - TLS CLient Profile = None
3. We recommend to change the configuration as follows
   - TLS Version in TLS 1.2
   - TLS Ciphers in Ignore
   - Peer Verification = Ignore
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>

Check : Server Flow Media Security Check

Instance	Target	Findings	Date & Time	Evidence
1	Trunk Gateway	Insecure media encryption.	02-01-2021 11:40:17	NA

Metadata

Risk category : Data Leaks	Security Policy: Insecure Media Configurations
Impact / Fallout : NA	Violation: NA

Description : Verify the media encryption related parameters are configured appropriately on the system

Recommendation :

1. We have observed the media is not encrypted to prevent data leaks for undefined.
2. Your current cofiguration is
   - Audio RTP Encryption = RTP
   - Audio Encrypted RTCP = undefined
   - Video RTP Encryption = RTP
   - Video Encrypted RTCP = undefined
3. It is highly recommended that the Encryption type in the MediaRules of the SBC is selected as SRTP. Ensure that all the preferred formats do not have RTP or NONE. Select a secured MediaRule on your server flow.
4. Configuration can be found at following navigate path "Network & Flows"=>"Server Flow"=>"

Check : Server Flow Signaling Interface Transport Check

Instance	Target	Findings	Date & Time	Evidence
1	Trunk Gateway	Insecured signaling interface.	02-01-2021 11:40:17	NA

Metadata

Risk category : Data Leaks	Security Policy: Insecure Signaling Configurations
Impact / Fallout : NA	Violation: NA

Description : Verify the signaling interface transport is TLS

Recommendation :

1. We have observed that insecured signaling interface is selected.
2. Your current cofiguration is
   - TLS Port = NaN
   - TCP Port = 5060
   - UDP Port = 5060
3. It is highly recommended that you select a secured signaling interface.
4. Configuration can be found at following navigate path "Network & Flows"=>"Server Flow"=>"

Check : CS_ASBCE_C016_1_6				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	Trunk Gateway	Insecured TLS Server security.	02-01-2021 11:40:17	NA

Metadata

Risk category : Data Leaks	Security Policy: Prevent information leaks through strong ciphers
Impact / Fallout : NA	Violation: NA

Description : Verify the TLS server profile parameters are configured appropriately on the system

Recommendation :

1. We have observed that the TLS Profile {"key":"NA"} is not securely cofigured.
2. Your current cofiguration is
   - TLS Server Profile = None
3. We recommend to change the configuration as follows
   - TLS Version in TLS 1.2
   - TLS Ciphers in Ignore
   - Peer Verification = Ignore
4. Configuration can be found at following navigate path "Network & Flows"=>"Server Flow"=>

Check : Backup Encryption Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	Backup Policy	Insecured backup encryption.	02-01-2021 11:40:17	NA

Metadata

Risk category : Alignment with Standards	Security Policy: Secured backup management
Impact / Fallout : NA	Violation: NA

Description : Verify the backup is encrypted appropriately

Recommendation :

1. We have observed that backup encryption is not sufficiently secured.
2. Your current cofiguration is Encryption Type = STATIC_KEY_ONLY
3. We recommend to change the values to either Static_Key_Password or Password_Only. Using the value of Static_Key only may increase the chance of compromise.
4. Configuration can be found at following navigate path "Monitoring & Logging"=>"SNMP"=>"SNMP V3"

Check : Local User Level and Status Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
2	Roles and privilege	Local users have administrator permissions	02-01-2021 11:40:17	NA

Metadata

Risk category : Alignment with Standards	Security Policy: Default account restrictions
Impact / Fallout : NA	Violation: NA

Description : Verify the role assignment for each local user is as expected.

Recommendation :

1. We have observed that local user listed below are assigned Service Administrator or System Administrator role.
   - User Name = ucsec, Role = System Administrator , Type = Local , Status = Normal
2. Disabled all the local users with Service Administrator and System Administrator and configure radius to secured admin access.

Check : Scrubber Rules Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	DoS protection	Appropriate Scrubber rule not enabled.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Whitelist Protections	
Impact / Fallout : NA			Violation: NA	
Description : Verify all the Scrubber rules are enabled with appropriate action				

Recommendation :

1. We have observed that scrubber rules are not appropriately configured.
2. Your current configuration is
   - Action = Alert
   - Status = Disabled
3. We recommend to change the values as following:
   - Action in Alert
   - Status = Enabled
4. Configuration can be found at following navigate path "SystemParameter"=>"Scrubber"=>"Packages".
5. If the package mentioned in the recommendation is not installed. Please install and enable the package".

Check : CAC Restrictions				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	Remote Worker	Inapproriate CAC restrictions.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient DoS/DDoS Restrictions	
Impact / Fallout : NA			Violation: NA	
Description : Verify the CAC restrictions are configured appropriately on the system				

Recommendation :

1. We have observed that CAC restrictions are not appropriately configured for {"key":"Application Rule Name = default"}.
2. Your current cofiguration is
   - Audio Inbound Restriction = true
   - Video Inbound Restriction = false
   - Audio Max Sessions Per Endpoint = 5
   - Video Max Sessions Per Endpoint =
3. It is advised to derive the parameters based on your network. We recommend to change the configuration as follows.
   - Audio Inbound Restriction = True
   - Video Inbound Restriction = True
   - Audio Max Sessions Per Endpoint = 10
   - Video Max Sessions Per Endpoint = 10
4. Configuration can be found at following navigate path "Network & Flows"=>"Subscriber Flow"=>

Check : Admission Control Restricted Remote Subnet Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	Trunk Gateway	Insecured access restrictions.	02-01-2021 11:40:17	NA
Metadata				
Risk category : DoS, DDoS and Cyber attacks			Security Policy: Insufficient Malformed Message Signature Restrictions	
Impact / Fallout : NA			Violation: NA	

Description : Verify the admission control value of remote subnet is configured appropriately on the system

Recommendation :

1. We have observed that remote subnet restrictions on the server flow are not appropriately configured.
2. Your current cofiguration is
   - Remote Subnet = *
3. We recommend to replace with the subnet from where you are expecting traffic.
4. Configuration can be found at following navigate path "Network & Flows"=>"Server Flow"=>

Check : Server Flow Check

Instance	Target	Findings	Date & Time	Evidence
1	Trunk Gateway	Other security parameters.	02-01-2021 11:40:17	NA

Metadata

Risk category : Data Leaks	Security Policy: Insecure Signaling Configurations
Impact / Fallout : NA	Violation: NA

Description : Verify the other security parameters are configured appropriately on the system

Recommendation :

1. We have observed that one of the additional security parameters have security concerns.
2. Your current cofiguration is
   - Routing Transport = Auto-Detect,UDP
   - Enable Natting = true
   - CDR Support = Off
3. We recommend to change the configuration as follows
   - Routing Transport in Ignore
   - Enable Natting = True
   - CDR Support in Radius,CDR_Adjunct
4. Configuration can be found at following navigate path "Network & Flows"=>"Server Flow"=>

Check : Server Flow CAC Check

Instance	Target	Findings	Date & Time	Evidence
1	Trunk Gateway	Inapproriate CAC restrictions.	02-01-2021 11:40:17	NA

Metadata

Risk category : DoS, DDoS and Cyber attacks	Security Policy: Insufficient DoS/DDoS Restrictions
Impact / Fallout : NA	Violation: NA

Description : Verify the CAC restrictions are configured appropriately on the system

Recommendation :

1. We have observed that CAC restrictions are not appropriately configured for {"key":"Application Rule Name = default"}.
2. Your current cofiguration is
   - Audio Inbound Restriction = true
   - Video Inbound Restriction = false
   - Audio Max Sessions Per Endpoint = 5
   - Video Max Sessions Per Endpoint =
3. It is advised to derive the parameters based on your network. We recommend to change the configuration as follows
   - Audio Inbound Restriction = True
   - Video Inbound Restriction = True
   - Audio Max Sessions Per Endpoint = 10
   - Video Max Sessions Per Endpoint = 10
4. Configuration can be found at following navigate path "Network & Flows"=>"Server Flow"=>

Check : Backup Schedule Configured Check				
Instance	**Target**	**Findings**	**Date & Time**	**Evidence**
1	NA	Backup schedule.	02-01-2021 11:40:17	NA
Metadata				
Risk category : Alignment with Standards			Security Policy: Secured backup management	
Impact / Fallout : NA			Violation: NA	
Description : Verify the backup is scheduled at regular interval				
Recommendation : 1. We have observed that backup schedule is not configured appropriately. 2. Your current cofiguration is Backup Frequency = NEVER 3. We recommend to configure backup schedules. 4. Configuration can be found at following navigate path "Monitoring & Logging"=>"SNMP"=>"SNMP V3"=>"Trap Severity Settings"				