Product Support Notice

PSN # PSN006077u

Original publication date: 08-July-2022. This is Issue #03, published date: 17-Aug-2022. Severity/risk level Medium Urgency When convenient

Name of problem

Hotfix-2 for SBCE release 8.1.3.1-38-21632

Products affected

Avaya Session Border Controller for Enterprise (ASBCE)

Versions: 8.1.3.1

Description

This Hotfix (sbce-8.1.3.1-39-22090-hotfix-06232022.tar.gz) addresses the following reported issues in the 8.1.3.1 GA release. This is a cumulative hotfix and includes the previous Hotfix/Mandatory patch fixes as well.

Note: *This patch is not qualified to be installed on DELL3240 hardware systems. If installed, it will cause grub corruption on DELL3240 servers and the only way to recover would be to rebuild the server.*

Jira No.	Issue Description
AURORA-29297	SBCE stops to send DNS requests.
AURORA-28999	ipcsipActiveTurnSessions in SIP Statistics is always zero.
AURORA-29402	Updated reset SNMP script.
AURORA-29404	Config API - Port range validation is missing in the Media interface api in the 8.1.2 release.
AURORA-29206	SBC config changes to support more sessions and additional A1 IP change for POM.
AURORA-27187	Outgoing PSTN calls in the hold, Re-INVITE is sent to the provider without Mediasec attributes.
AURORA-28840	SNMP Problem: ssyndi crash due to memory leak within oampserver process.
AURORA-28944	SBCE not sending CANCEL messages and generating new INVITE.
AURORA-29411	Recording stop in long SIPrec call and SBC responded 481 error msg when SIPrec sends UPDATE msg.
AURORA-29474	Changes in the typical profile required as per customer security policy are not working.
AURORA-28374	One-way Audio for a blind Transfer from Aura User1 to Aura User2 for a Teams Call.
AURORA-29535	Security package update RHSA-2022:5052, RHSA-2022:4642, RHSA-2022:2213, RHSA-2022:2191, RHSA-2022:1487, RHSA-2022:1440, RHSA-2022:1198, RHSA-2022:1069, RHSA-2022:1066, RHSA-2022:0666, RHSA-2021:4785
AURORA-29498	After transfer in NG911 with AMR-WB codec, the voice between caller and 911 operator becomes garbled.
AURORA-29443	Core files generated on SBCE lead to unexpected more fallow.
AURORA-29497	Call transfer failed with "481 Call Does Not Exist (no call-id match and message have local tag)".

Following Fixes carried from Hotfix-1 (sbce-8.1.3.1-39-21939-hotfix-05042022.tar.gz)

Jira No.	Issue Description
AURORA-28505	tracesbc is not showing the initial inbound call leg from MS Teams on calls view
AURORA-28100	Calls not connecting via SBC for MS Teams Users
AURORA-28941	sysmon is down due to 0 byte certificate(couldn't able to read) or a wrong certificate present
AURORA-28702	TEAMS Interop - Transfer CLID Issues
AURORA-29012	incomplete video session in SDP in reINVITE msg cause SBC to crash (Teams)
AURORA-29166	Security concerns for CVE-2022-0778 and RHSA-2022:1066

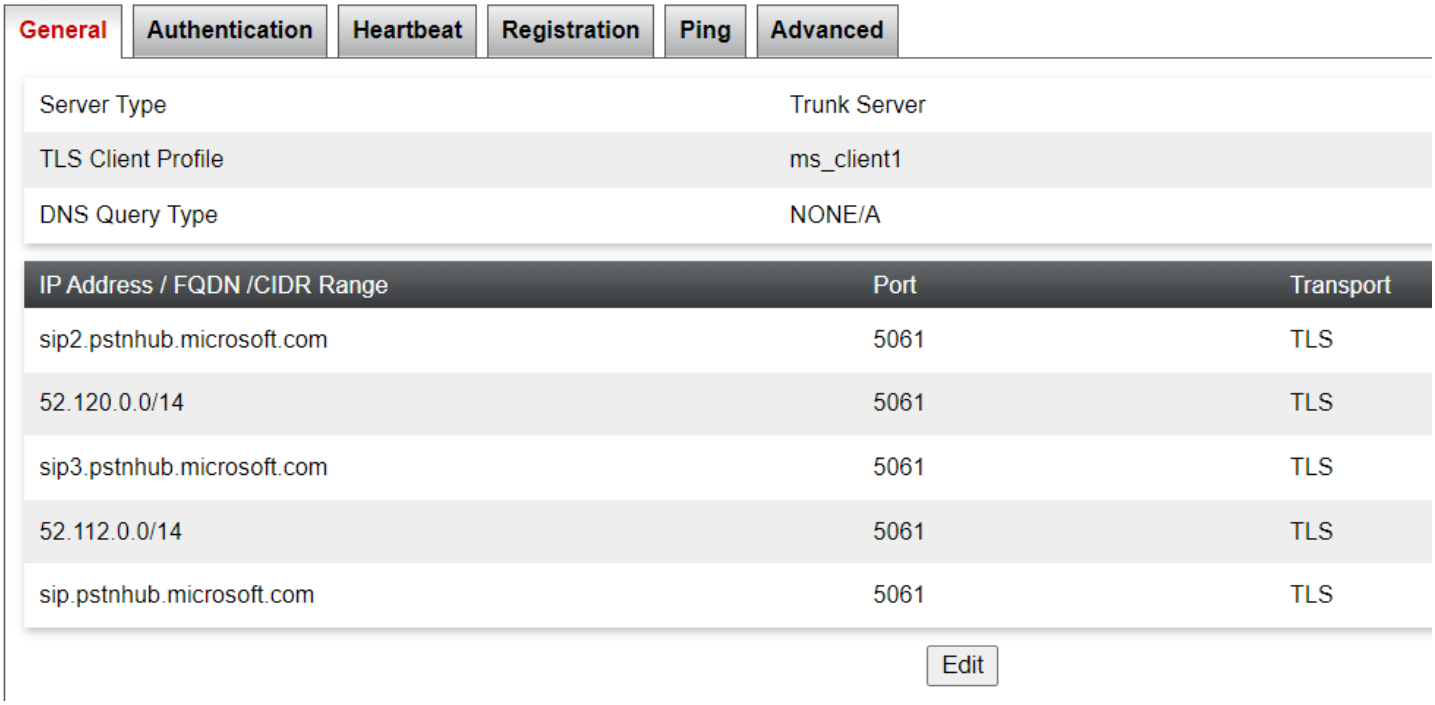
AURORA-29202	Security package update RHSA-2022:1066, RHSA-2022:0621, RHSA-2022:0620, RHSA-2022:0609, RHSA-2022:0473, RHSA-2022:0306, RHSA-2022:0204
AURORA-28944	SBCE not sending CANCEL messages and generating new INVITE
AURORA-28534	Resolve memory leak due to dns_result_t
AURORA-29006	Feature development for allowing CIDR range
AURORA-28644	Intermittent one-way audio when Re-Invite is received from carrier (Telus)
AURORA-28881	Blind Transfer from Aura User1 to Aura User2 is not working with MS Teams User using ICE Gateway Disable and Aura Side RTP when ICE Enable
AURORA-29265	Observe a lot of xMS errors in debug log
AURORA-29279	SSYNDI Crash
AURORA-29241	Qualys scan causes SBC to crash
AURORA-29200	[Security][Critical] RCE vulnerability in Spring MVC/WebFlux
AURORA-27781	Partition /archive is full 100% because OAMPSvr.log is 98 GB in size
AURORA-27095	turncontroller PID: CPU Utilization exceeded more than the max 90

In addition to the above fixes, CIDR support has been added in hotfix-1:

With this, the CIDR range is added to the "Trunk Server" configuration profile (Services->SIP Servers) along with the IP address and FQDN. By configuring CIDR in SIP Server, the inbound calls from all the IP addresses in the CIDR block will be allowed by the ASBCE. The CIDR will not be used for routing outbound calls.

For example, in the case of Microsoft direct routing, the inbound calls to ASBCE can be from any of the IP addresses from the CIDR blocks 52.112.0.0/14 and 52.120.0.0/14. By configuring these CIDRs along with Direct Routing Server FQDNs, the SBC will no longer reject the inbound call if the call is from one of the IP addresses in the CIDR block. The outbound calls will still route to the resolved FQDN addresses.

Below is the reference snapshot of the MS team's server config with CIDR configured.



Resolution

Important: Install the patch during a maintenance window to avoid service disruption.

The patch is to be installed on the 8.1.3.1-38-21632 version.

Install the patch on both EMS and SBCE servers.

File name: sbce-8.1.3.1-39-22090-hotfix-06232022.tar.gz
md5sum: cd50e29369049ff3e6da6e3a1c52fc52
PLDS Download ID: SBCE0000311

Workaround or alternative remediation

N/A

Remarks

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Take a backup of ASBCE and save it on external storage.

Download

Download the patch from https://plds.avaya.com
Download ID: SBCE0000311

Patch install instructions Service-interrupting? Y

Important: Install the patch during a maintenance window to avoid service disruption.
The patch needs to be applied to both EMS and SBC(s). (version: 8.1.3.1-38-21632)
Note: For HA SBCE, first install the patch on the secondary SBCE and perform failover. Later, install the patch on the new Secondary SBCE.

1. Copy the patch file to /home/ipcs directory on SBCE(s) using any SFTP client for example WINSCP.
2. Login to the CLI of SBCE as user ipcs.
3. Switch user to root with the command:
   su – root
4. Change directory to /home/ipcs with the command:
   cd /home/ipcs
5. Verify md5sum of the patch file matches with the md5sum on PLDS i.e. cd50e29369049ff3e6da6e3a1c52fc52
   Command:
   md5sum sbce-8.1.3.1-39-22090-hotfix-06232022.tar.gz
6. Untar the patch file:
   Command:
   tar –zxvf sbce-8.1.3.1-39-22090-hotfix-06232022.tar.gz
7. Go to directory sbce-8.1.3.1-39-22090-hotfix-06232022
   cd sbce-8.1.3.1-39-22090-hotfix-06232022
8. Stop the application using the command.
   /etc/init.d/ipcs-init stop
9. Run install_hotfix.sh script:
   sh install_hotfix.sh
10. Once the script is run successfully, reboot the SBCE/EMS
    /sbin/reboot

Verification

NA

Failure

NA

Does Patch uninstall instructions Service-interrupting?

Note: For HA SBCEs, uninstall the patch first on secondary SBCE, and perform failover. Later, uninstall the patch on the new Secondary SBCE.
Important: Make sure to uninstall the patch during a maintenance window to avoid service disruption.

1. Login to the CLI of SBCEs as user ipcs.
2. Switch user to root:

su – root

3. Go to directory /home/ipcs/sbce-8.1.3.1-39-22090-hotfix-06232022 with the command:
   cd /home/ipcs/sbce-8.1.3.1-39-22090-hotfix-06232022
4. Stop the application using the command:
   /etc/init.d/ipcs-init stop
5. Uninstall the patch.
   sh remove_hotfix.sh
6. Once the script is run successfully, reboot the SBCE/EMS
   /sbin/reboot

Note: patch uninstall will roll back the RPMs to the GA version. You must re-install any other patch if installed previously.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks
N/A
Avaya Security Vulnerability Classification
Not Susceptible
Mitigation
N/A

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya Support Terms of Use.