Product Support Notice

PSN # PSN006023u

Original publication date: 03-Mar-2022. This is Issue: #01, published date: 03-Mar-2022.

Severity/risk level Medium Urgency When convenient

Name of problem

Resolving FQDNs connection for Microsoft Teams

Products affected

Avaya Session Border Controller for Enterprise 8.1.x, 10.x

Problem description

We are seeing some connectivity problems with Microsoft Team Service when connecting via the following FQDNs

1. sip.pstnhub.microsoft.com --> primary
2. sip2.pstnhub.microsoft.com --> secondary
3. sip3.pstnhub.microsoft.com --> tertiary

Microsoft Teams gets a forbidden 403 from ASBCE when it sends an invite to it from an IP that it hasn't resolved explicitly for sip,sip2, and sip3.pstnhub.microsoft.com

Resolution

The use of sip-all.pstnhub.microsoft.com appears to resolve most of the cases. Avaya is working on implementing a feature that allows for specific subnets to be recognized as Teams traffic.

Workaround or alternative remediation

After discussion with Microsoft, Microsoft recommends the use of sip-all.pstnhub.microsoft.com for connectivity to Teams cloud.

We recommend to add the FQDN sip-all.pstnhub.microsoft.com below the 3 primary FQDNs above:

1. sip.pstnhub.microsoft.com --> primary
2. sip2.pstnhub.microsoft.com --> secondary
3. sip3.pstnhub.microsoft.com --> tertiary
4. sip-all.pstnhub.microsoft.com

For DoD and Office 365 high environments, we recommend to use the following domain names as mentioned in the Microsoft link:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns

Remarks

n/a

Patch Notes

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

Backup before applying the patch

N.A

Download	
N.A	
Patch install instructions	Service-interrupting?
N.A	No
Verification	
N.A	
Failure	
N.A	
Patch uninstall instructions	
N.A	

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.