Product Notice #0539

Response to RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS) for AudioCodes' SBCs, Media Gateway and MSBRs

Vulnerability Details

On July 7, 2024, security researchers disclosed the following vulnerability in the RADIUS protocol: "CVE-2024-3596: RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. This vulnerability may impact any RADIUS client and server."

Affected Products

The following AudioCodes products are affected by this vulnerability:

- Mediant Software and Hardware Session Border Controllers (SBCs)
- Mediant Gateway
- Mediant MSBR
- MediaPack

Mitigations

Blast-RADIUS is a protocol vulnerability, and thus affects all RADIUS implementations using non-EAP authentication methods over UDP.

AudioCodes plans to provide an updated RADIUS client that will resolve the vulnerability in an upcoming software version. This will be announced in the relevant device's Release Notes.

Note: Full mitigation of CVE-2024-3596 may require updating your RADIUS server.

As an immediate step, it's recommended to implement one of the following mitigations:

- If available, use other and more secured authentication protocols such as OAuth 2.0 or LDAP.
- If RADIUS authentication is still required, make sure that the connection between the device and RADIUS server is on an isolated internal network.

Announcement Date

July 31, 2024.

If you have any questions, at https://www.audiocodes.com/corporate/offices-worldwide

AudioCodes Ltd. | 6 Ofra Haza Street | Naimi Park | Or Yehuda | Israel | +972-3-976-4000