Title	CVE-2022-3602, CVE-2022-3786: OpenSSL Buffer overrun triggered in X.509 certificate verification
Security Advisory Number	17
Affected Product(s)	None
TAC Reference	N/A
Audience	Operations, Customers, Partners
Date	8th November 2022
Supersede	Yes
Severity	Low - Not Affected

Background:

Two high security alerts (CVE-2022-3602, CVE-2022-3786) have been issued for OpenSSL where a buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking.

For further information regarding CVE-2022-3602 and CVE-2022-3786 please refer to:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3602

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3786

Next Steps:

Speakerbus has assessed both alerts and can confirm that none of the products listed below are affected by CVE-2022-3602 and CVE-2022-3786, because they either **do not** use OpenSSL or **do not** use OpenSSL versions that are exposed to the vulnerability:

- iManager Centralised Management System (iCMS)
- iManager Web Server (iWS)
- iManager Call Data Server (iCDS)
- iManager Gateway Server (iGS)
- iManager CloudBase (iCB)
- iManager Communications Server (iCS)
- Voice Conference Manager (VCM)
- SB 534 System
- All Speakerbus Endpoints and Gateways

Speakerbus provide applications that may be installed on customer provided servers which may have other applications installed. Speakerbus cannot comment on other software that may be running on these servers, however Speakerbus applications either **do not** use OpenSSL or **do not** use OpenSSL versions affected by CVE-2022-3602 and CVE-2022-3786.

If you have any questions regarding this communication, please contact Speakerbus Global Customer Support (https://www.speakerbus.com/helpdesk).

End of Security Advisory 17.