Speakerbus

Security Advisory

CVE-2023-0286

SA Number	18
Affected Product(s)	N/A
TAC Reference	29797
Audience	Operations, Customers, Partners
Date	2nd March 2023
Supersede	N/A
Severity	Low – Not Affected

Background

A high security alert (CVE-2023-0286) has been issued for OpenSSL where type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. This vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

For further information regarding CVE-2023-0286 please refer to:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0286

Next Steps

Speakerbus has assessed this alert and can confirm we have not implemented our own functionality for retrieving CRLs over a network and are not impacted by CVE-2023-0286 for the products listed:

- iManager Gateway Server (iGS)
- iManager CloudBase (iCB)
- iManager Communications Server (iCS)
- 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 are not impacted by CVE-2023-0286.

Note: Other Speakerbus products not listed do not use OpenSSL

End of security advisory.