Title	CVE-2021-44228: Apache Log4j 2 Vulnerability
Security Advisory Number	14
Affected Product(s)	None
TAC Reference	N/A
Audience	Operations, Customers, Partners
Date	13th December 2021
Supersede	N/A
Severity	Low - Not Affected

Background:

A serious security alert (CVE-2021-44228) has been issued for a remote code execution vulnerability in the Apache-Log4j 2 library. Apache Log4j 2 is an open-source Java logging library developed by the Apache Foundation. For further information regarding CVE-2021-44228 please refer to:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Next Steps:

Speakerbus has assessed this vulnerability and can confirm the following products **do not** use Apache Log4j 2 and are not vulnerable to CVE-2021-44228:

- 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 **do not** use Apache Log4j 2 and are not vulnerable to CVE-2021-44228.

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

End of Security Advisory 14.