Security Advisory 011

CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 and CVE-2019-11091

Issued Thursday, 16th May 2019

Updated Wednesday, 26th February 2020

Microarchitectural Data Sampling (MDS) Vulnerabilities: CVE-2018-12126 (Fallout), CVE-2018-12127, CVE-2018-12130 (Ridl, Zombieload) and CVE-2019-11091
A number of flaws in Intel microprocessors have been identified which could allow sensitive information to be accessed. More information can be found at: https://access.redhat.com/security/vulnerabilities/mds.

All Speakerbus products have protection from these vulnerabilities. Providing the following conditions are met:

Those installed on Windows Servers need to have been patched with Microsoft patched with Microsoft's May 14 Monthly Rollup or later. These products are:

- iManager Centralised Management System (iCMS),
- iManager Call Data Server (iCDS),
- SB 534 GA Server and System Controllers
- Voice Conference Manager (VCM) products.
- ARIA iManager Web Server (iWS)

Those installed on CentOS Servers need to be updated to the following versions:

- iManager Communication Server (iCS) – v2.625 or later – see AN0117
- iManager Gateway Server (iGS) - v1.201 or later – see AN0119
- ARIA iManager CloudBase (iCB) v1.430 or later – see AN0135

For further information please contact your regional partner or our service desk.
http://www.speakerbus.com/support/