

Product Security Vulnerability Report – LPC#4

Subject

Non-compliance to *hopIncrement* in Bluetooth specification

Dialog Product Category

Connectivity > Bluetooth low energy

Vulnerability Reference

3rd party reported as a specification non-compliance, not declared in any vulnerability database.

Vulnerability Description

In the Bluetooth specification, for data channel selection algorithm for CSA #1 (Channel Selection Algorithm #1), the *hopIncrement* should be a random value in the range 5 to 16. This value is specified by the central device (LE master) through *Hop* field. In Dialog's products, while operating as peripheral device (LE slave), the implementation permits a *hopIncrement* of less than 5. Allowing *hopIncrement* to be less than 5, narrows the channel frequency hopping and may cause congestion on the frequency spectrum.

Impact

If the central device (LE master) sets the *Hop* field to zero and the devices connected are configured to use CSA #1, then the channel frequency used for connection events will not hop and all transmissions will use the same frequency potentially jamming the system if that particular frequency has interference. This could result in bad or failed Bluetooth communication.

In customer products, where Dialog's product is co-located with another 2.4 GHz wireless technology that does not support Adaptive Frequency Hopping, it may result in Denial of Service.

Dialog Response Summary

Analysis has been conducted by the Product Security Incident Response Team (PSIRT) and the reported specification non-compliance has been verified by Dialog Engineering. All of Dialog's Bluetooth low energy products are impacted.

Interoperability testing by Dialog has not identified any mobile phone (100's checked) that specified a *Hop* field of value less than 5. As such, the non-compliance to *hopIncrement* has no direct impact for products in the field. The non-compliance to *hopIncrement* could be exposed by a malicious attacker that could lead to bad or failed Bluetooth communication in environments where there is interference on that channel frequency or Denial of Service on the co-located 2.4 GHz wireless technology.

The PSIRT assessment is that this incident constitutes a low risk and fixes will be provided accordingly.

Product Mitigation

<i>Product</i>	<i>SDK</i>	<i>impact</i>	<i>hotfix</i>	<i>available</i>	<i>SDK fix</i>	<i>available</i>
DA14531	SDK6	low	hotfix for SDK6.0.14	15-Jul	TBD	TBD
DA14580	SDK3	low	none	-	none	-
	SDK5	low	none	-	none	-
DA14581	SDK3	low	none	-	none	-
	SDK5	low	none	-	none	-
DA14583	SDK3	low	none	-	none	-
	SDK5	low	none	-	none	-
DA14585	SDK6	low	hotfix for SDK6.0.14	15-Jul	TBD	TBD
DA14585-00T	SDK6	low	hotfix for SDK6.0.14	15-Jul	TBD	TBD
DA14586	SDK6	low	hotfix for SDK6.0.14	15-Jul	TBD	TBD
DA14680	SDK1	low	none	-	none	-
DA14681-01	SDK1	low	none	-	none	-
DA14682	SDK1	low	hotfix for SDK1.0.14	15-Jul	TBD	TBD
DA14683	SDK1	low	hotfix for SDK1.0.14	15-Jul	TBD	TBD
DA14691	SDK10	low	none	-	SDK10.0.10	27-Jul
DA14695	SDK10	low	none	-	SDK10.0.10	27-Jul
DA14697	SDK10	low	none	-	SDK10.0.10	27-Jul
DA14699	SDK10	low	none	-	SDK10.0.10	27-Jul

Note: TBD = SDK version & date are to be determined.

Fix Availability

SDK & hotfix releases will be posted to the SDK section of the appropriate product page on the Dialog website.

Access to hotfixes is conditional to the standard SW License Agreement (SLA).

Contact

If you have any information regarding Dialog product security vulnerabilities, please write to PSIRT@diasemi.com (in English).

For general support questions please contact the support forum:
<https://support.dialog-semiconductor.com/forum>

Revision History

Revision	Date	Description
1	<2-July-2020>	Initial version.

Disclaimer

Unless otherwise agreed in writing, the Dialog Semiconductor products (and any associated software) referred to in this document are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of a Dialog Semiconductor product (or associated software) can reasonably be expected to result in personal injury, death or severe property or environmental damage. Dialog Semiconductor and its suppliers accept no liability for inclusion and/or use of Dialog Semiconductor products (and any associated software) in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Information in this document is believed to be accurate and reliable. However, Dialog Semiconductor does not give any representations or warranties, express or implied, as to the accuracy or completeness of such information. Dialog Semiconductor furthermore takes no responsibility whatsoever for the content in this document if provided by any information source outside of Dialog Semiconductor.

Dialog Semiconductor reserves the right to change without notice the information published in this document, including, without limitation, the specification and the design of the related semiconductor products, software and applications. Notwithstanding the foregoing, for any automotive grade version of the device, Dialog Semiconductor reserves the right to change the information published in this document, including, without limitation, the specification and the design of the related semiconductor products, software and applications, in accordance with its standard automotive change notification process.

Applications, software, and semiconductor products described in this document are for illustrative purposes only. Dialog Semiconductor makes no representation or warranty that such applications, software and semiconductor products will be suitable for the specified use without further testing or modification. Unless otherwise agreed in writing, such testing or modification is the sole responsibility of the customer and Dialog Semiconductor excludes all liability in this respect.

Nothing in this document may be construed as a license for customer to use the Dialog Semiconductor products, software and applications referred to in this document. Such license must be separately sought by customer with Dialog Semiconductor.

All use of Dialog Semiconductor products, software and applications referred to in this document is subject to Dialog Semiconductor's [Standard Terms and Conditions of Sale](#), available on the company website (www.dialog-semiconductor.com) unless otherwise stated.

Dialog, Dialog Semiconductor and the Dialog logo are trademarks of Dialog Semiconductor Plc or its subsidiaries. All other product or service names and marks are the property of their respective owners.

© 2020 Dialog Semiconductor. All rights reserved.