Product Security Vulnerability Report – LPC#5

Subject

“Impersonation in the Passkey Entry Protocol” vulnerability

Dialog Product Category

Connectivity > Bluetooth low energy

Vulnerability Reference

Research published in a paper by ANSSI titled “Testing for weak key management in Bluetooth Low Energy implementations”.

Bluetooth SIG statement regarding the ‘Impersonation in the Passkey Entry Protocol’ Vulnerability.

Declared as CVE-2020-26558

Vulnerability Description

The ANSSI paper describes how LE Secure connections pairing with Passkey authentication procedure can be subjected to a man-in-the-middle (MITM) attack. An attacker has to be in the vicinity of the initiating and responding devices at the time of pairing. The attacker impersonates the initiator by reflecting the genuine responses, establishing the attacker as an initiator to the responder. In order for the attack to succeed it has to attack all 20 times involving 20 bits of the 6-digit Passkey during the Passkey authentication procedure. The attacker does not succeed in impersonating the responder by this method, preventing a fully transparent MITM attack on the pairing procedure between the initiator and responder.

This attack exposes a vulnerability in the Bluetooth specification, it is not an implementation vulnerability.

Impact

Once the MITM attacker is acknowledged by the responding device as a credible initiator, the responder will be authenticated to the attacker rather than the initiator, permitting the attacker to act in the role of an encrypted and authenticated initiator. Both the application data on logical connection and GATT services can be accessed by the attacker. In cases where the responder supports GATT client role, the attacker can manipulate the GATT service characteristics. In cases where the responder supports GATT server role, the attacker accesses the GATT service characteristics.

Dialog Response Summary

Analysis has been conducted by the Product Security Incident Response Team (PSIRT) and the reported specification vulnerability has been verified by Dialog Engineering. All of Dialog's Bluetooth low energy products that support LE Secure Connections are impacted.

The PSIRT assessment is that this incident constitutes a medium risk (with CVSS rating 4.6) and an SDK fix roll-out will be conducted according to use-case severity.

The Dialog fix design will follow the guidance from Bluetooth SIG.

Product Mitigation

Product	*SDK*	*Impacted*	*SDK fix*	*available*
DA14530	SDK6	Y	6.0.16	Q3-2021
DA14531	SDK6	Y	6.0.16	Q3-2021
DA14580	SDK3	N	not applicable	
	SDK5	N	not applicable	
DA14581	SDK3	N	not applicable	
	SDK5	N	not applicable	
DA14583	SDK3	N	not applicable	
	SDK5	N	not applicable	
DA14585	SDK6	Y	6.0.16	Q3-2021
DA14585-00T	SDK6	Y	6.0.16	Q3-2021
DA14586	SDK6	Y	6.0.16	Q3-2021
DA14680	SDK1	Y	to be decided	
DA14681-01	SDK1	Y	to be decided	
DA14682	SDK1	Y	to be decided	
DA14683	SDK1	Y	to be decided	
DA14691	SDK10	Y	10.0.12	Q4-2021
DA14695	SDK10	Y	10.0.12	Q4-2021
DA14697	SDK10	Y	10.0.12	Q4-2021
DA14699	SDK10	Y	10.0.12	Q4-2021

Notes:

1. the SDK1 fix plan will be defined once the use-case severity has been determined.
2. "not impacted" products do not support LE Secure Connections so the vulnerability does not exist. Therefore an SDK fix is not applicable.

Fix Availability

SDK's will be posted to the Resources section of the appropriate product page on the Dialog website.

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	<16-June 2021>	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.