# XBee Zigbee on S2C hardware - Keys can be sent in the clear

**Digi International Security Notice**

**Transport Key sent "In the Clear"**

Digi International Security Notice

October 9, 2019

**Overview**

The purpose of this notice is to inform our customers of a security vulnerability regarding a potential inadvertent transmission of the Network Key "in the clear". Through a vulnerability in enabling the NULL transport key, a node without the appropriate pre-configured link key but who was once securely associated with the network could be allowed back onto the secured network using an incorrect pre-configured link key. This node could then pass the network key "in the clear" to other nodes attempting to join the network through the affected node.

This notice informs our end users of the vulnerability, which devices are impacted, what steps users can perform to mitigate the risk and to inform you of what Digi is doing to fix this issue. This vulnerability can only be exploited by a node internal to the network. The node must already be part of the network, or have once securely joined to the network for the network to be vulnerable. Thus, Digi has rated the ability to exploit this vulnerability as **MEDIUM**.

**Affected Products**

The vulnerability is limited to products containing Digi XBee S2C Zigbee and Digi XBee S2D Zigbee devices. The following products are impacted:

- Digi XBee S2B Zigbee-based products
- Digi XBee S2C Zigbee
- Digi XBee S2D Zigbee
- Digi XBee S2C Zigbee adapters
- Digi XBee S2C Zigbee Gateway/Digi XBee S2C Zigbee Industrial Gateway

Note: if you have questions on any Digi products and services not listed, contact us at +1 (952) 912-3456, or via the web site at www.digi.com/support.

**Unaffected Products**

This vulnerability is not present in the following Zigbee products:

- Digi XBee 3 Zigbee 3.0

**Detailed Information on Affected Products**

The possibility exists that a node on a distributed or trust center-based network which had joined the network with a pre-configured link key could be compromised. With serial access to the node, it can be removed from the network and could then be allowed to join the network again with a link key of 0, if the network has the NULL transport key enabled by default. When joining, the NULL transport key is sent containing the network key to the node when it joins. This enables nodes from outside of the network to join the encrypted network through the errant node because the network key is transferred to the remote node through the use of the NULL transport key which was sent by the affected node. The NULL transport key is enabled by default. Only networks that have not specifically disabled the NULL transport key (DO bit 3) and have nodes with serial access inside a secured network are vulnerable.

**Origin of the NULL Transport Key**

The introduction of the NULL transport key support was to be used when a network does not send keys in the clear but needs compatibility with specific legacy devices running an old Zigbee stack that does not support pre-configured link keys. Digi does not anticipate that customers will need this feature and will disable this feature by default on Digi XBee Zigbee S2C releases. Starting with firmware version 4061 the NULL transport key will be disabled by default by setting bit 3 of the DO parameter.

**Risk**

This vulnerability can only be exploited with serial access to a node once associated with the encrypted network. The node would need to be misconfigured with the link key of 0 in order to expose this vulnerability. A node that has never associated with the secured network and has never been issued the pre-configured link key is not at risk of exposing the network key to a third party. In the field, Digi sees the ability to exploit this vulnerability as MEDIUM. The risk, however, needs to be determined by the end-user and how they have chosen to deploy devices within their environment, and who might have access to those devices.

**Suggested Steps to Protect Your Network**

The analysis shows that once a router joins with proper settings, the router's address is stored in the coordinator's address table. Thereafter, the NULL transport key can trigger a joining router with misconfigured parameters to transmit the network key, allowing it to join the network.

To reduce the possibility of exposure to this vulnerability:

1. Set bit 3 of the DO (Device Options) parameter to disable the NULL transport key on the coordinator when the network is formed.
- Note: Changing the ATDO setting on the network organizer will require network re-establishment. Take care when moving the existing network to the new one. There are various strategies to do this. One option is:

- Use the ATNR1 command to send a broadcast transmission, causing all devices in the network to leave and migrate to a different PAN. Open the join window using NJ. Then, set DO=8, and wait for devices to join.

2. Set ATKY as one of the first parameters, and immediately write that parameter. This will reduce the risk of an error during the configuration process leaving the link key in a misconfigured state, but will not completely mitigate the vulnerability.

   Following best security practices, Digi will be closing this vulnerability on Digi XBee Zigbee S2C modules by:

- Setting bit 3 of the DO parameter to disable the transmission of the NULL transport key by default.
- The KY parameter will now indicate if it has been set to a non-default value, indicating that a valid pre-configured link key is being used.
- Setting bit 3 of the DO parameter on a router will not cause a network leave to occur. Changes to note that changing the DO value on a coordinator after the network is formed will still cause the network to reform. Also of note, changing the DO value on any Digi XBee S2C Zigbee device on firmware 4060 or earlier will cause that node to leave the network.