

## Information note

**Topic** TOBY-L2 / MPC-I-L2 Security advisory document

UBXDOC-686885345-1825 C1-Public

**Author** Drazen Drinic

**Date** 06-Oct-2023

Copying, reproduction, modification, or disclosure to third parties of this document or any part thereof is only permitted with the express written permission of u-blox. The information contained herein is provided "as is" and u-blox assumes no liability for its use. No warranty, either express or implied, is given, including but not limited to the accuracy, correctness, reliability, and fitness for a particular purpose of the information. This document may be revised by u-blox at any time. For most recent documents, visit [www.u-blox.com](http://www.u-blox.com).  
Copyright© u-blox AG.

### 1 Affected products

Product name	Ordering code	Type number	Firmware
TOBY-L200	TOBY-L200-03S	TOBY-L200-03S-01 / MPC-I-L200-03S-01	16.19 A01.02, 16.19 A01.04
MPC-I-L200	MPC-I-L200-03S	TOBY-L200-03S-02 / MPC-I-L200-03S-02	17.00 A01.00
		TOBY-L200-03S-03 / MPC-I-L200-03S-03	17.00 A01.01
	TOBY-L200-03A	TOBY-L200-03A-01	16.19 A01.02, 16.19 A01.04
		TOBY-L200-03A-02	17.00 A01.00
		TOBY-L200-03A-03	17.00 A01.01
TOBY-L210	TOBY-L210-03S	TOBY-L210-03S-01 / MPC-I-L210-03S-01	16.19 A01.02, 16.19 A01.04
MPC-I-L210	MPC-I-L210-03S	TOBY-L210-03S-02 / MPC-I-L210-03S-02	17.00 A01.00
		TOBY-L210-03S-03 / MPC-I-L210-03S-03	17.00 A01.01
	TOBY-L210-03A	TOBY-L210-03A-01	16.19 A01.02, 16.19 A01.04
		TOBY-L210-03A-02	17.00 A01.00
		TOBY-L210-03A-03	17.00 A01.01
TOBY-L280	TOBY-L280-03S	TOBY-L280-03S-01 / MPC-I-L280-03S-01	16.19 A01.02, 16.19 A01.04
MPC-I-L280	MPC-I-L280-03S	TOBY-L280-03S-02 / MPC-I-L280-03S-02	17.00 A01.00
		TOBY-L280-03S-03 / MPC-I-L280-03S-03	17.00 A01.01
	TOBY-L280-03A	TOBY-L280-03A-01	16.19 A01.02, 16.19 A01.04
		TOBY-L280-03A-02	17.00 A01.00
		TOBY-L280-03A-03	17.00 A01.01

### 2 Type

- |  |   |
|--|---|
| <input type="checkbox"/> Product status change     | <input type="checkbox"/> Documentation update         |
| <input type="checkbox"/> Hardware/component change | <input type="checkbox"/> Certification information    |
| <input type="checkbox"/> Firmware/software update  | <input checked="" type="checkbox"/> Security advisory |
| <input type="checkbox"/> Label change              | <input type="checkbox"/> Other                        |

### 3 Description



CVE-2023-0011 Security vulnerability issue has been identified on the products in the table above. The vulnerability allows a potential malicious attacker to execute system commands in privileged environment. This vulnerability can be exploited only when a potential attacker is connected to the serial interface of the modem over wired connection (has physical access to the module). Only in that case the attacker can issue commands to the module. This security vulnerability affects only the device that is subject of the attack (to which attacker is physically connected) and cannot be exploited to affect entire fleet of devices.

## 4 Schedule

N/A.

## 5 Customer impact and recommended action

- To prevent the malicious attacker to carry out such attacks, physical access to the module shall be allowed to authorized users only.
- Because TOBY-L2 / MPC1-L2 series products are in end-of-life, customers are advised to migrate to new products such as LARA-R6 and LARA-L6 series modules.

## 6 Related documentation

- [1] TOBY-L2 / MPC1-L2 series modules end of life notification, [UBX-21048767](#)
- [2] LARA-R6 00B-01 mass production information note, [UBX-23004170](#)
- [3] LARA-L6004(D) 00B mass production information note, [UBX-23003246](#)