OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

TBOX-SA-2021-0005

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0005
- **Vulnerability** : CVE-2021-22642
- **Publisher** : Ovarro (vendor)
- **Contact** : cybersecurity@ovarro.com

- **Current status** : final
- **Current version** : 1.0
- **Initial release date** : 23 March 2021
- **Current release date** : 23 March 2021

Revision History

Version	Date	Description
1.0	23 March 2021	First version

Vulnerability

The TBox may crash when receiving specially crafted Modbus packets.

Vulnerable Products

This vulnerability affects TBox MS-CPU32, TBox MS-CPU32-S2, TBox LT2, TBox TG2, TBox RM2 product families in version **1.45 and earlier** of the firmware.

Solution

A new version of firmware have been released fixing this issue.
This fix is available only for all affected products and is available in version **1.46 or later** of the firmware.

Workaround

There are no workaround available for this vulnerability.

Releases

New software version can be downloaded from our web site www.ovarro.com in "Customer Support" section (service portal).

General Security Recommendations

There is a document explaining the best practices to keep the TBox secured. It can be downloaded from our web site www.ovarro.com in "Customer Support" section (service portal, manual, "TBox Cybersecurity_Best Practice").

Acknowledgment

Ovarro thanks the following parties for their efforts:

- Uri Katz at Claroty for identifying and reporting this

OVARRO
CONNECTING TECHNOLOGIES