OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

TBOX-SA-2021-0008

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0008
- **Vulnerability** : CVE-2021-22644
- **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

A attacker may connect through SSH and execute illegitimate shell commands as a standard user (non-root).

Vulnerable Products

This vulnerability affects LT2 / RM2 / TG2 / CPU32 / CPU32-S2 product families in firmware **1.44 and earlier**.

Solution

A first aspect of the solution is explained in **TBOX-SA-2021-0004** as the provided solution will forbid any unauthenticated user through Modbus protocol to gain SSH access.

Then, a new version of firmware which filters correctly illegitimate commands have been released.
This fix is available only for all affected products and is available in version **1.45 or later** of the firmware.

So we advise to update to a version **1.46 or later** of the firmware and to enable authentication based on a user list (other authentication mechanism are legacy and not secure enough) for the Modbus protocol.

Workaround

There are no workaround available for this vulnerability.

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