PUBLIC

Security Advisory

TBOX-SA-2026-0001

14 July 2026

Revision History

Version	Date	Description
1	07/07/2026	Initial Release

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2026-0001
- **CVE Reference**: -
- **CVSS Score**: 7.2
- **Publisher**: Ovarro
- **Contact**: cybersecurity@ovarro.com
- **Current Status**: Final
- **Current Version**: 1
- **Initial Release Date**: 14/07/2026
- **Latest Release Date**: 14/07/2026

2 Vulnerability

An attacker with a passive man-in-the-middle position can decrypt the encrypted login password from Modbus TCP communications. This might give sufficient access level to reprogram the TBox.

3 Vulnerable Products

This vulnerability affects LT2 / TG2 / CPU32 / CPU32-S2 product families in firmware **1.51 and earlier**.

4 Solution

A new version of TWinSoft (**13.0**) has been released including a new firmware **2.00** which enforce to use Modbus over HTTPS Web Socket for remote communication and application updates, ensuring the password cannot be intercepted. Therefore, it is not necessary anymore to leave Modbus TCP enabled. It is advised to block Modbus TCP port with internal firewall unless it is used for another purpose (e.g. Monitoring).

CPU32 product is not maintained anymore as mentioned in EOL document and no mitigation is available.
It is advised to update to CPU32-S2.

5 Releases

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

6 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").

7 Acknowledgment

Ovarro thanks the following parties for their efforts:

- Limes Security for identifying and reporting this