



PUBLIC

Security Advisory

TBOX-SA-2024-0001

21 November 2024

Revision History

Version	Date	Description
1	21/11/2024	Initial Release

1 Executive Summary

- **Document Type:** Security Advisory
- **Reference:** TBOX-SA-2024-0001
- **CVE Reference:** -
- **CVSS Score:** 8.6
- **Publisher:** Ovarro
- **Contact:** cybersecurity@ovarro.com
- **Current Status:** Final
- **Current Version:** 1
- **Initial Release Date:** 21/11/2024
- **Latest Release Date:** 21/11/2024

2 Vulnerability

The affected TBox RTUs may push a malicious script onto the TBox firewall configuration to acquire root privileges.

3 Vulnerable Products

This vulnerability affects LT2 / RM2 / TG2 / CPU32 / CPU32-S2 product families in firmware **1.50 and earlier**.

4 Solution

A new version of TWinSoft (**12.8**) has been released including a new firmware **1.51.631** which prevent to inject code into firewall configuration.

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