PUBLIC

Security Advisory

TBOX-SA-2023-0003

21 November 2024

Revision History

Version	Date	Description
1	29/06/2023	Initial Release
2	21/11/2024	Update of affected versions

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2023-0003
- **Vulnerabilities**: CVE-2023-36609
- **Severity**: High
- **Publisher**: Ovarro
- **Contact**: cybersecurity@ovarro.com
- **Current Status**: Final
- **Current Version**: 1
- **Initial Release Date**: 29/06/2023
- **Latest Release Date**: 21/11/2024

2 Vulnerability

The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host 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 setup user defined configuration scripts.

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:

- Floris Hendriks and Jeroen Wijenbergh of Radboud University for identifying and reporting this
- Limes Security for identifying and reporting the effectiveness of the mitigation