PUBLIC

Security Advisory

TBOX-SA-2023-0002

29 June 2023

Revision History

Version	Date	Description
1	29/06/2023	Initial Release

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2023-0002
- **Vulnerabilities**: CVE-2023-36607
- **Severity**: Medium
- **Publisher**: Ovarro
- **Contact**: cybersecurity@ovarro.com
- **Current Status**: Final
- **Current Version**: 1
- **Initial Release Date**: 29/06/2023
- **Latest Release Date**: 29/06/2023

2 Vulnerability

TBox is missing authorization for running some API commands. An attacker running these commands could reveal sensitive information such as software versions and web server file contents.

3 Vulnerable Products

This vulnerability affects LT2 / RM2 / TG2 / CPU32 / CPU32-S2 product families in firmware **between 1.46 and 1.50.598**.

4 Solution

A new version of TWinSoft (**12.7.2**) has been released including a new firmware **1.50.599** which is not using revealing sensitive information to unauthenticated requests.

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