PUBLIC

Security Advisory

TBOX-SA-2023-0004

29 June 2023

The document contains confidential and proprietary information of Ovarro Limited, its subsidiaries and affiliated companies and must be kept strictly confidential. It may not be disclosed in whole or in part under any circumstances without the express prior written consent of Ovarro Limited.

Revision History

Version	Date	Description
1	29/06/2023	Initial Release

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2023-0004
- **Vulnerabilities**: CVE-2023-36610, CVE-2023-36611
- **Severity**: High
- **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

An insufficient entropy and improper authorization is set on a token being used for authentication. An attacker may exploit the vulnerabilities to gain access to an user account having access to application source code.

3 Vulnerable Products

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

4 Workaround

The workaround against this vulnerability is to disable the SSH access through the integrated firewall and to disable the user account SSH access by emptying its password in application. Setting a password on application will also make the exploit useless as the retrieved application will be encrypted.

5 Solution

A new version of TWinSoft (**12.7.2**) has been released including a new firmware **1.50.599** which fix entropy and file permissions.

6 Releases

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

7 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”).

8 Acknowledgment

Ovarro thanks the following parties for their efforts:

- Floris Hendriks and Jeroen Wijenbergh of Radboud University for identifying and reporting this