PUBLIC

Security Advisory

TBOX-SA-2023-0001

29 June 2023

Revision History

Version	Date	Description
1	29/06/2023	Initial Release

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2023-0001
- **Vulnerabilities**: CVE-2023-36608
- **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

Use of a Broken or Risky Cryptographic Algorithm - TBox stores hashed passwords using MD5 encryption, which is an insecure encryption algorithm. An attacker could connect to the TBox and gain system user account password.

3 Vulnerable Products

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

Note that in firmware version **1.44 and earlier,** a high privileged user account password can be gained. In later version that user account password in disabled making this vulnerability less critical.

4 Workaround

The workaround against this vulnerability is to disable the SSH access through the integrated firewall or disable the user account SSH access by emptying its password in application.

5 Solution

A new version of TWinSoft (**12.7.2**) has been released including a new firmware **1.50.599** which is not using MD5 as algorithm. It also disable system user accounts password.

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