PUBLIC

Security Advisory

TBOX-SA-2023-0005

29 June 2023

Revision History

Version	Date	Description
1	29/06/2023	Initial Release

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2023-0005
- **Vulnerabilities**: CVE-2023-3395
- **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

TWinSoft configuration tool store sensitive information as plaintext in memory. An attacker with access to the application source could obtain plaintext password of SSH user account and engineer user accounts.

3 Vulnerable Products

All TWinSoft version are affected.

4 Workaround

The workaround against this vulnerability is to set a document password so that only intended person can load the document.

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