OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

TBOX-SA-2021-0006

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0006
- **Vulnerability** : CVE-2021-22646
- **Publisher** : Ovarro (vendor)
- **Contact** : cybersecurity@ovarro.com

- **Current status** : final
- **Current version** : 1.0
- **Initial release date** : 23 March 2021
- **Current release date** : 23 March 2021

Revision History

Version	Date	Description
1.0	23 March	First version

Vulnerability

A attacker may send and install malicious package to the TBox by using proprietary Modbus functions used for package update.

Vulnerable Products

This vulnerability affects LT2 / RM2 / TG2 / CPU32 / CPU32-S2 product families in firmware **1.44 and earlier**.

Solution

A first aspect of the solution is explained in **TBOX-SA-2020-0004** and will prevent to send files into the TBox without being authenticated with the highest access level.

Another aspect of the solution is to configure the TBox to accept to install only packages coming from a trusted computer. This is done by signing all the packages that will be sent to the TBox with a certificate, which must be present into the TBox for verification. The functionality is available from version **1.44 or later** of the firmware, and **12.3 or later** of TWinSoft.

We advise the user to update to version **1.46 or later** of firmware, and **12.4 or later** of TWinSoft, and to enable package signature functionality.

Workaround

By enabling user protection, only user having the highest access level will be able to send the install command of packages that were being sent. This make this attack as a race condition as the malicious package must be sent during a legitimate update sequence.

Releases

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

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").

Acknowledgment

Ovarro thanks the following parties for their efforts:

- Uri Katz at Claroty for identifying and reporting this

Copyright © 2021 Ovarro SA. ALL RIGHTS RESERVED.

Copyright in the whole and every part of this document belongs to Ovarro SA ('the Owner') and may not be used, sold, transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any person other than in accordance with the terms of the Owner's agreement or otherwise without the prior written consent of the Owner.

OVARRO
CONNECTING TECHNOLOGIES