OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

TBOX-SA-2021-0004

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0004
- **Vulnerability** : CVE-2020-28990, CVE-2021-22648
- **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 2021	First version

Vulnerability

Sensitive file from the file system of the TBox may be read or written, even without authenticating first.

Vulnerable Products

This vulnerability affects the following products :

- Legacy product families : TBox MS-CPU16, TBox LT, TBox TG, TBox RM, TBox LP, TBox WM (all firmware versions)
- Current product families : TBox MS-CPU32, TBox MS-CPU32-S2, TBox LT2, TBox TG2, TBox RM2 (firmware version **1.45 and earlier**)

Solution

Current product families

A new firmware release is done which protect the access to the file system into the TBox. Only the files that may be read or written by configuration software will be accessible with the right access level.
It implies to have user authentication enabled to have a fully protected system.

Impacted customers are then advised to enable authentication based on a user list (other authentication mechanism are legacy and not secure enough) and to use firmware version **1.46 or later**.

Legacy product families

Customers using a legacy product are advised to contact local sales representative to update to an equivalent product family.

Workaround

There are no workaround available for this vulnerability.

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:

- Reid Wightman at Dragos for identifying and reporting this
- Uri Katz at Claroty for identifying and reporting this

OVARRO
CONNECTING TECHNOLOGIES