OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

TBOX-SA-2021-0003

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0003
- **Vulnerability** : CVE-2020-28989
- **Publisher** : Ovarro (vendor)
- **Contact** : cybersecurity@ovarro.com

- **Current status** : final
- **Current version** : 1.0
- **Initial release date** : 05 Feb 2021
- **Current release date** : 05 Feb 2021

Revision History

Version	Date	Description
1.0	05 Feb 2021	First version

Vulnerability

There is a buffer overflow vulnerability in the webserver.

Vulnerable Products

The vulnerability is present into the legacy products families, with all firmware versions.

- TBox MS-CPU16
- TBox LT
- TBox TG
- TBox RM
- TBox LP
- TBox WM

Solution

There will be no fixes available for this vulnerability as it impacts only legacy products.
We advise impacted customers to contact local sales representative to update to an equivalent product family.

Workaround

There are no workaround available for this vulnerability.

Acknowledgment

Ovarro thanks the following parties for their efforts:

- Reid Wightman at Dragos for identifying and reporting this

OVARRO
CONNECTING TECHNOLOGIES