OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

TBOX-SA-2021-0010

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0010
- **Vulnerability** : -
- **Publisher** : Ovarro (vendor)
- **Contact** : cybersecurity@ovarro.com

- **Current status** : final
- **Current version** : 1.0
- **Initial release date** : 30 Aug 2021
- **Current release date** : 30 Aug 2021

Revision History

Version	Date	Description
1.0	30 Aug 2021	First version

Vulnerability

A vulnerability has been found in the Linux kernel file system which could allow an attackers to gain root privileges access. This vulnerability is named **Sequoia** and has been published recently through **CVE-2021-33909**. Whilst the currently published exploit does not affect our products due to its limited memory size, the vulnerability remains present.

Vulnerable Products

This vulnerability affects **MS-CPU32-S2** and **LT2** products running a Linux kernel version **4.9.264 or earlier**.

Solution

A new version of TWinSoft (**12.5**) has been released.
It includes a new Linux kernel (version **4.9.279**) that fixes this vulnerability.

Workaround

The workaround against this vulnerability is to disable the SSH access through the integrated firewall.

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").

OVARRO
CONNECTING TECHNOLOGIES