



Security Advisory

TBOX-SA-2021-0009

Summary

- **Document Type** : Security Advisory
- **Id** : TBOX-SA-2021-0009
- **Vulnerability** : CVE-2021-22650
- **Publisher** : Ovarro (vendor)
- **Contact** : cybersecurity@ovarro.com

- **Current status** : final
- **Current version** : 1.1
- **Initial release date** : 30 Aug 2021
- **Current release date** : 1st Feb 2022

Revision History

Version	Date	Description
1.0	30 Aug 2021	First version
1.1	1 st Feb 2022	Explicit the attack vector in description

Vulnerability

A remote attacker could update the source project file (TPG) stored into the TBox by a malicious one so that code could be executed on machine executing TWinSoft when an engineer download it.

Vulnerable Products

This vulnerability affects TWinSoft releases **12.4 and earlier**.

Solution

A first aspect of the solution is explained in **TBOX-SA-2021-0004** as the provided solution will forbid any unauthenticated user to update source project file into the TBox.

A new version of TWinSoft have also been released to avoid code execution. It will now extract the source project files exclusively to the output directory, whatever the location of the referenced files were when the source project file was created.

So we advise to update to a version **12.5 or later** of TWinSoft.

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:

- Uri Katz at Clarity for identifying and reporting this

Copyright © 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.

