



# CVE-2022-47386

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-47386
<b>State</b>	PUBLIC
<b>Assigner</b>	info@cert.vde.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-15 10:15:00 UTC
<b>Updated</b>	2023-05-22 19:55:00 UTC
<b>Description</b>	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Codesys</a>	<a href="#">Control For Beaglebone SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Empc-a/imx6 SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Iot2000 SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Linux SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Pfc100 SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Pfc200 SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Plcnext SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Raspberry Pi SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control For Wago Touch Panels 600 SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control Rte For Beckhoff Cx SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control Rte SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control Runtime System Toolkit</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Control Win SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Development System V3</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Hmi SI</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Safety Sil2 Psp</a>	All	All	All	All
Application	<a href="#">Codesys</a>	<a href="#">Safety Sil2 Runtime Toolkit</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://customers.codesys.com/index.php">customers.codesys.com/index.php</a>	MISC	<a href="https://customers.codesys.com">customers.codesys.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)