CVE-2022-47381

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-47381
State	PUBLIC
Assigner	info@cert.vde.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-15 10:15:00 UTC
Updated	2023-05-22 19:36:00 UTC
Description	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in multiple CODESYS products i

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
customers.codesys.com/index.php	MISC	customers.codesys.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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