CVE-2022-22519

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

Summary

CVE	CVE-2022-22519
State	PUBLIC
Assigner	info@cert.vde.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-07 19:15:00 UTC
Updated	2022-05-10 15:22:00 UTC
Description	A remote, unauthenticated attacker can send a specific crafted HTTP or HTTPS requests causing a buffer over-read resulti

Risk And Classification

Problem Types: CWE-126

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 Beckhoff Cx9020	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 SI	All	All	All	All
Application	Codesys	Control Rte SI For Beckhoff Cx	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	All	All	All	All
Application	Codesys	Embedded Target Visu Toolkit	All	All	All	All
Application	Codesys	Hmi SI	All	All	All	All

Application	Codesys	Remote Target Visu 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.

Legacy QID Mappings

590918 ABB AC500 Multiple Vulnerabilities (ABBVREP0075)

591091 3S-Smart CodeSYS V3 Multiple Vulnerabilities (Advisory 2022-07)

591168 3S-Smart CodeSYS V3 Buffer Over-Read Vulnerability (Advisory 2022-07 Version: 3.0)