



CVE-2021-34593

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

Summary

CVE	CVE-2021-34593
State	PUBLIC
Assigner	info@cert.vde.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-26 10:15:00 UTC
Updated	2022-04-12 18:05:00 UTC
Description	In CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56 unauthenticated crafted invalid requ

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codesys	Plcwinnt	All	All	All	All
Application	Codesys	Runtime Toolkit	All	All	All	All
Application	Codesys	Runtime Toolkit	All	All	All	All

References

Reference	Source	Link	Tags
WAGO 750-8xxx PLC Denial Of Service / User Enumeration ≈ Packet Storm	MISC	packetstormsecurity.com	
customers.codesys.com/index.php	CONFIRM	customers.codesys.com	
Full Disclosure: SEC Consult SA-20211028-0 :: Denial of Service in CODESYS V2	FULLDISC	seclists.org	
CODESYS 2.4.7.0 Denial Of Service ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Steffen Robertz and Gerhard Hechenberger from the SEC Consult Vulnerability Lab.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)