



CVE-2018-20026

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

Summary

CVE	CVE-2018-20026
State	PUBLIC
Assigner	vulnerability@kaspersky.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-19 21:29:00 UTC
Updated	2023-03-29 18:40:00 UTC
Description	Improper Communication Address Filtering exists in CODESYS V3 products versions prior V3.5.14.0.

Risk And Classification

Problem Types: NVD-CWE-noinfo

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 Beaglebone SI	All	All	All	All
Application	Codesys	Control For Empc-a/imx6 SI	All	All	All	All
Application	Codesys	Control For Empc-a/imx6 SI	All	All	All	All
Application	Codesys	Control For Empc-a/imx6 SI	All	All	All	All
Application	Codesys	Control For lot2000 SI	All	All	All	All
Application	Codesys	Control For lot2000 SI	All	All	All	All
Application	Codesys	Control For Linux 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 Pfc100 SI	All	All	All	All
Application	Codesys	Control For Pfc200 SI	All	All	All	All
Application	Codesys	Control For Pfc200 SI	All	All	All	All
Application	Codesys	Control For Raspberry Pi SI	All	All	All	All
Application	Codesys	Control For Raspberry Pi SI	All	All	All	All
Application	Codesys	Control Rte 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 Rte SI For Beckhoff Cx	All	All	All	All
Application	Codesys	Control Rte SI For Beckhoff Cx	All	All	All	All
Application	Codesys	Control Runtime Toolkit	All	All	All	All
Application	Codesys	Control Runtime Toolkit	All	All	All	All
Application	Codesys	Control Win SI	All	All	All	All
Application	Codesys	Control Win SI	All	All	All	All
Application	Codesys	Development System V3	All	All	All	All
Application	Codesys	Development System V3	All	All	All	All
Application	Codesys	Gateway	All	All	All	All
Application	Codesys	Gateway	All	All	All	All
Application	Codesys	Hmi SI	All	All	All	All
Application	Codesys	Hmi SI	All	All	All	All
Application	Codesys	Opc Server	All	All	All	All
Application	Codesys	Opc Server	All	All	All	All
Application	Codesys	Plchandler	All	All	All	All
Application	Codesys	Plchandler	All	All	All	All
Application	Codesys	Safety Sil2	All	All	All	All
Application	Codesys	Safety Sil2	All	All	All	All
Application	Codesys	Targetvisu SI	All	All	All	All
Application	Codesys	Targetvisu SI	All	All	All	All

References

Reference	Source	Link
3S-Smart Software CODESYS ICSA-18-352-04 Multiple Security Vulnerabilities	BID	www.securityfocus.com/bid/101111
3S-Smart Software Solutions GmbH CODESYS V3 Products CISA	MISC	ics-cert.us-cert.gov/alerts/ICS-18-036
KLCERT-18-036: CodeSYS Control V3 Improper Communication Address Filtering Kaspersky ICS CERT	MISC	ics-cert.kaspersky.com/alerts/ICS-18-036
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#)