



CVE-2019-18858

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2019-18858
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-20 18:15:00 UTC
Updated	2019-11-22 16:51:00 UTC
Description	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codesys	Control For Beaglebone	All	All	All	All
Application	Codesys	Control For Beaglebone	All	All	All	All
Application	Codesys	Control For Empec-a/imx6	All	All	All	All
Application	Codesys	Control For Empec-a/imx6	All	All	All	All
Application	Codesys	Control For Empec-a/imx6	All	All	All	All
Application	Codesys	Control For lot2000	All	All	All	All
Application	Codesys	Control For lot2000	All	All	All	All
Application	Codesys	Control For Linux	All	All	All	All
Application	Codesys	Control For Linux	All	All	All	All
Application	Codesys	Control For Pfc100	All	All	All	All
Application	Codesys	Control For Pfc100	All	All	All	All
Application	Codesys	Control For Pfc200	All	All	All	All
Application	Codesys	Control For Pfc200	All	All	All	All
Application	Codesys	Control For Plcnext	All	All	All	All
Application	Codesys	Control For Plcnext	All	All	All	All
Application	Codesys	Control For Raspberry Pi	All	All	All	All
Application	Codesys	Control For Raspberry Pi	All	All	All	All

Application	Codesys	Control Rte	All	All	All	All
Application	Codesys	Control Rte	All	All	All	All
Application	Codesys	Control Runtime System Toolkit	All	All	All	All
Application	Codesys	Control Runtime System Toolkit	All	All	All	All
Application	Codesys	Control Win	All	All	All	All
Application	Codesys	Control Win	All	All	All	All
Application	Codesys	Embedded Target Visu Toolkit	All	All	All	All
Application	Codesys	Embedded Target Visu Toolkit	All	All	All	All
Application	Codesys	Hmi	All	All	All	All
Application	Codesys	Hmi	All	All	All	All
Application	Codesys	Remote Target Visu Toolkit	All	All	All	All
Application	Codesys	Remote Target Visu Toolkit	All	All	All	All

References

Reference	Source	Link	Tag
customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-10_CDS-68...	MISC	customers.codesys.com	Ven
CODESYS V3 Unauthenticated Remote Heap Buffer Overflow - Research Advisory Tenable®	MISC	www.tenable.com	Exp
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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](https://www.tenable.com) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.tenable.com).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report