



CVE-2021-34586

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

Summary

CVE	CVE-2021-34586
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	2021-10-28 18:01:00 UTC
Description	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests may cause a Null pointer dereference in the

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codesys	Codesys	All	All	All	All

References

Reference	Source	Link	Tags
customers.codesys.com/index.php	CONFIRM	customers.codesys.com	
CODESYS V2 Web Server Multiple Vulnerabilities - Research Advisory Tenable®	MISC	www.tenable.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability was discovered by Tenable Research.

Legacy QID Mappings

[591219](#) 3S-Smart CODESYS GmbH v2 Multiple Vulnerabilities (Advisory 2021-15 Version: 4.0)

© [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](#)