



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 lot2000 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) |

© [CVE.report](https://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.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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