# CVE-2019-18858

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## 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 Empc-a/imx6 | All | All | All | All |
| Application | Codesys | Control For Empc-a/imx6 | All | All | All | All |
| Application | Codesys | Control For Empc-a/imx6 | All | All | All | All |
| Application | Codesys | Control For Iot2000 | All | All | All | All |
| Application | Codesys | Control For Iot2000 | 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.