# CVE-2017-17317

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-17317 |
| **State** | PUBLIC |
| **Assigner** | psirt@huawei.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2018-07-02 13:29:00 UTC |
| **Updated** | 2018-08-24 13:57:00 UTC |
| **Description** | Common Open Policy Service Protocol (COPS) module in Huawei USG6300 V100R001C10; V100R001C20; V100R001C3 |

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Huawei | Dp300 | - | All | All | All |
| Hardware | Huawei | Dp300 | - | All | All | All |
| Operating System | Huawei | Dp300 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Dp300 Firmware | v500r002c00 | All | All | All |
| Hardware | Huawei | Rp200 | - | All | All | All |
| Hardware | Huawei | Rp200 | - | All | All | All |
| Operating System | Huawei | Rp200 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Rp200 Firmware | v600r006c00 | All | All | All |
| Operating System | Huawei | Rp200 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Rp200 Firmware | v600r006c00 | All | All | All |
| Hardware | Huawei | Te30 | - | All | All | All |
| Hardware | Huawei | Te30 | - | All | All | All |
| Operating System | Huawei | Te30 Firmware | v100r001c02 | All | All | All |
| Operating System | Huawei | Te30 Firmware | v100r001c10 | All | All | All |
| Operating System | Huawei | Te30 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te30 Firmware | v600r006c00 | All | All | All |
| Operating System | Huawei | Te30 Firmware | v100r001c02 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Huawei | Te30 Firmware | v100r001c10 | All | All | All |
| Operating System | Huawei | Te30 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te30 Firmware | v600r006c00 | All | All | All |
| Hardware | Huawei | Te40 | - | All | All | All |
| Hardware | Huawei | Te40 | - | All | All | All |
| Operating System | Huawei | Te40 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te40 Firmware | v600r006c00 | All | All | All |
| Operating System | Huawei | Te40 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te40 Firmware | v600r006c00 | All | All | All |
| Hardware | Huawei | Te50 | - | All | All | All |
| Hardware | Huawei | Te50 | - | All | All | All |
| Operating System | Huawei | Te50 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te50 Firmware | v600r006c00 | All | All | All |
| Operating System | Huawei | Te50 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te50 Firmware | v600r006c00 | All | All | All |
| Hardware | Huawei | Te60 | - | All | All | All |
| Hardware | Huawei | Te60 | - | All | All | All |
| Operating System | Huawei | Te60 Firmware | v100r001c01 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v100r001c10 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v600r006c00 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v100r001c01 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v100r001c10 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v500r002c00 | All | All | All |
| Operating System | Huawei | Te60 Firmware | v600r006c00 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Security Advisory - Buffer Overflow Vulnerability in Some Huawei Products | CONFIRM | www.huawei.com | Vendor Advisory |
| 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.

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

**Free CVE JSON API** cve.report/api

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