# CVE-2017-10940

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-10940 |
| **State** | PUBLIC |
| **Assigner** | zdi-disclosures@trendmicro.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-10-31 19:29:00 UTC |
| **Updated** | 2019-10-09 23:21:00 UTC |
| **Description** | This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Joyent Smart Data Center |

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Joyent | Triton Datacenter | - | All | All | All |
| Application | Joyent | Triton Datacenter | - | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Zero Day Initiative | MISC | zerodayinitiative.com | Third Party |
| Security Advisory: ZDI-CAN-3853 (Docker File Overwrite) Vulnerability – Joyent Support | CONFIRM | help.joyent.com | Vendor Adv |
| Joyent Triton DataCenter CVE-2017-10940 Privilege Escalation Vulnerability | BID | www.securityfocus.com | Third Party |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, a |

No vendor comments have been submitted for this CVE.

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

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