# CVE-2018-16738

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2018-16738 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2018-10-10 21:29:00 UTC |
| **Updated** | 2023-11-07 02:53:00 UTC |
| **Description** | tinc 1.0.30 through 1.0.34 has a broken authentication protocol, although there is a partial mitigation. This is fixed in 1.1. |

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Starwindsoftware | Starwind Virtual San | v8 | build12533 | All | All |
| Application | Starwindsoftware | Starwind Virtual San | v8 | build12658 | All | All |
| Application | Tinc-vpn | Tinc | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| www.tinc-vpn.org Git - tinc/commit | | www.tinc-vpn.org | |
| Debian -- Security Information -- DSA-4312-1 tinc | DEBIAN | www.debian.org | Third Party Advisory |
| CVE-2018-16738 tinc vulnerability in StarWind VSAN for vSphere (VSA) | MISC | www.starwindsoftware.com | |
| security | CONFIRM | tinc-vpn.org | Vendor Advisory |
| www.tinc-vpn.org Git - tinc/commit | CONFIRM | www.tinc-vpn.org | Mailing List, Mitigation, |
| 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

| | |
|---|---|
| 500704 | Alpine Linux Security Update for tinc |
| 504475 | Alpine Linux Security Update for tinc |
| 690261 | Free Berkeley Software Distribution (FreeBSD) Security Update for tinc (a4eb38ea-cc06-11e8-ada4-408d5cf35399) |