# CVE-2001-1316

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2001-1316 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2001-07-16 04:00:00 UTC |
| **Updated** | 2017-12-19 02:29:00 UTC |
| **Description** | Buffer overflows in Teamware Office Enterprise Directory allows remote attackers to cause a denial of service (crash) and p |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Teamware | Teamware Office | 5.0 | All | All | All |
| Application | Teamware | Teamware Office | 5.1 | All | All | All |
| Application | Teamware | Teamware Office | 5.2 | All | All | All |
| Application | Teamware | Teamware Office | 5.3 | All | All | All |
| Application | Teamware | Teamware Office | 5.4 | All | All | All |
| Application | Teamware | Teamware Office | 5.0 | All | All | All |
| Application | Teamware | Teamware Office | 5.1 | All | All | All |
| Application | Teamware | Teamware Office | 5.2 | All | All | All |
| Application | Teamware | Teamware Office | 5.3 | All | All | All |
| Application | Teamware | Teamware Office | 5.4 | All | All | All |

## References

| Reference | Sourc |
|---|---|
| Teamware Information for VU#688960 | CONF |
| IBM X-Force Exchange | XF |
| L-116 | CIAC |
| www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3 | MISC |

| | |
|---|---|
| Teamware Office LDAP Buffer Overflow Vulnerabilities | BID |
| CERT Advisory CA-2001-18 Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP) | CERT |
| CERT/CC Vulnerability Note VU#688960 | CERT- |
| CVE Program record | CVE.C |
| NVD vulnerability detail | NVD |

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**