



# CVE-2008-2943

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2008-2943                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2008-06-30 21:41:00 UTC                                                                                                     |
| <b>Updated</b>         | 2017-08-08 01:31:00 UTC                                                                                                     |
| <b>Description</b>     | Double free vulnerability in IBM Tivoli Directory Server (TDS) 6.1.0.0 through 6.1.0.15 allows remote authenticated adminis |

## Risk And Classification

### Problem Types: CWE-399

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                 | Version  | Update | Edition | Language |
|-------------|--------|-------------------------|----------|--------|---------|----------|
| Application | ibm    | Tivoli Directory Server | 6.1.0.0  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.1  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.10 | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.11 | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.12 | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.13 | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.14 | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.15 | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.2  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.3  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.4  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.5  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.6  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.7  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.8  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.9  | All    | All     | All      |
| Application | ibm    | Tivoli Directory Server | 6.1.0.0  | All    | All     | All      |

|             |                     |                                         |          |     |     |     |
|-------------|---------------------|-----------------------------------------|----------|-----|-----|-----|
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.1  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.10 | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.11 | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.12 | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.13 | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.14 | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.15 | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.2  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.3  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.4  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.5  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.6  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.7  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.8  | All | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Tivoli Directory Server</a> | 6.1.0.9  | All | All | All |

| References                                                                                      |  |         |                                              |
|-------------------------------------------------------------------------------------------------|--|---------|----------------------------------------------|
| Reference                                                                                       |  | Source  | Link                                         |
| IBM Tivoli Directory Server Double-Free Vulnerability - Advisories - Secunia                    |  | SECUNIA | <a href="#">secunia.com</a>                  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                |  | VUPEN   | <a href="#">www.vupen.com</a>                |
| IBM Tivoli Directory Server Adding 'ibm-globalAdminGroup' Entry Denial of Service Vulnerability |  | BID     | <a href="#">www.securityfocus.com</a>        |
| IBM IO09113: TDS Server ABEND adding ibm-globalAdminGroup entry                                 |  | AIXAPAR | <a href="#">www-1.ibm.com</a>                |
| IBM X-Force Exchange                                                                            |  | XF      | <a href="#">exchange.xforce.ibmcloud.com</a> |
| CVE Program record                                                                              |  | CVE.ORG | <a href="#">www.cve.org</a>                  |
| NVD vulnerability detail                                                                        |  | NVD     | <a href="#">nvd.nist.gov</a>                 |

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)