



# CVE-2000-0547

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2000-0547                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | cve@mitre.org                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2000-06-09 04:00:00 UTC                                                                                                    |
| <b>Updated</b>         | 2021-02-02 17:57:00 UTC                                                                                                    |
| <b>Description</b>     | Buffer overflow in Kerberos 4 KDC program allows remote attackers to cause a denial of service via the localrealm variable |

## Risk And Classification

### Problem Types: CWE-120

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                                          | Product                                 | Version | Update  | Edition | Language |
|-------------|-------------------------------------------------|-----------------------------------------|---------|---------|---------|----------|
| Application | <a href="#">Cygnus Network Security Project</a> | <a href="#">Cygnus Network Security</a> | -       | All     | All     | All      |
| Application | <a href="#">Cygnus Network Security Project</a> | <a href="#">Cygnus Network Security</a> | -       | All     | All     | All      |
| Application | <a href="#">Kerbnet Project</a>                 | <a href="#">Kerbnet</a>                 | -       | All     | All     | All      |
| Application | <a href="#">Kerbnet Project</a>                 | <a href="#">Kerbnet</a>                 | -       | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos</a>                | All     | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos</a>                | 4.0     | -       | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos</a>                | 4.0     | patch10 | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos</a>                | All     | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos</a>                | 4.0     | -       | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos</a>                | 4.0     | patch10 | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos 5</a>              | 1.1     | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos 5</a>              | 1.1.1   | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos 5</a>              | 1.1     | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos 5</a>              | 1.1.1   | All     | All     | All      |
| Application | <a href="#">Mit</a>                             | <a href="#">Kerberos 5</a>              | All     | All     | All     | All      |

## References

| Reference                                                                          | Source  | Link                                                               |
|------------------------------------------------------------------------------------|---------|--------------------------------------------------------------------|
| web.mit.edu/kerberos/www/advisories/krb4kdc.txt                                    | CONFIRM | <a href="http://web.mit.edu">web.mit.edu</a>                       |
| Kerberos4 KDC AUTH_MSG_KDC_REQUEST NULL termination Vulnerability                  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>   |
| 20000609 Security Advisory: MULTIPLE DENIAL OF SERVICE VULNERABILITIES IN KRB4 KDC | BUGTRAQ | <a href="http://archives.neohapsis.com">archives.neohapsis.com</a> |
| DoS Vulnerabilities in Kerberos 4 KDC Programs                                     | CIAC    | <a href="http://ciac.llnl.gov">ciac.llnl.gov</a>                   |
| CERT Advisory CA-2000-11 MIT Kerberos Vulnerable to Denial-of-Service Attacks      | CERT    | <a href="http://www.cert.org">www.cert.org</a>                     |
| CVE Program record                                                                 | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                       |
| NVD vulnerability detail                                                           | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                     |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

**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)