

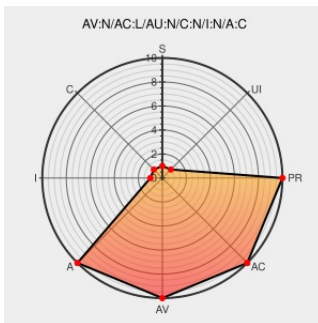


CVE-2011-1527

Published on: 10/20/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:16 PM UTC

CVE-2011-1527

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Kerberos 5](#) from [Mit](#) contain the following vulnerability:

The kdb_ldap plugin in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.9 through 1.9.1, when the LDAP back end is used, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a kinit operation with incorrect string case for the realm, related to the is_principal_in_realm, krb5_set_error_message, krb5_ldap_get_principal, and process_as_req functions.

CVE-2011-1527 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
US-CERT Vulnerability Note VU#659251 - Multiple MIT KRB5 KDC daemon vulnerabilities	US Government Resource www.kb.cert.org text/html	CERT-VN VU#659251
#629558 - krb5-kdc: kdb_ldap plugin crashes during kinit "user@DOMAIN" with wrong case for "DOMAIN" - Debian Bug report logs	bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=629558
Support / Security / Advisories // MDVSA-2011:159 Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2011:159
Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2011:1379

Vendor Advisory

web.mit.edu

text/plain



CONFIRM

web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-006.txt

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos 5	1.9	All	All	All
Application	Mit	Kerberos 5	1.9.1	All	All	All
Application	Mit	Kerberos 5	1.9	All	All	All
Application	Mit	Kerberos 5	1.9.1	All	All	All
cpe:2.3:a:mit:kerberos_5:1.9:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.9.1:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.9:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.9.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023 |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)