



CVE-2011-0282

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2011-0282
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-10 18:00:00 UTC
Updated	2020-01-21 15:46:00 UTC
Description	The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.6.x through 1.9, when an LDAP backend is used, allows

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos	5-1.6.3	All	All	All
Application	Mit	Kerberos	5-1.6.3	All	All	All
Application	Mit	Kerberos 5	1.6	All	All	All
Application	Mit	Kerberos 5	1.6.1	All	All	All
Application	Mit	Kerberos 5	1.6.2	All	All	All
Application	Mit	Kerberos 5	1.7	All	All	All
Application	Mit	Kerberos 5	1.7.1	All	All	All
Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All
Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	All	All	All
Application	Mit	Kerberos 5	1.9	All	All	All
Application	Mit	Kerberos 5	1.6	All	All	All
Application	Mit	Kerberos 5	1.6.1	All	All	All
Application	Mit	Kerberos 5	1.6.2	All	All	All
Application	Mit	Kerberos 5	1.7	All	All	All
Application	Mit	Kerberos 5	1.7.1	All	All	All

Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All
Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	All	All	All
Application	Mit	Kerberos 5	1.9	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
MIT Kerberos KDC Principal Name LDAP Request NULL Pointer Denial Of Service Vulnerability	BID	www.securityfocus.com
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:004	SUSE	lists.opensuse.org
SecurityFocus	BUGTRAQ	www.securityfocus.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Kerberos Multiple Denial of Service Vulnerabilities - Secunia.com	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Security Advisory SA43273 - Red Hat update for krb5 - Secunia	SECUNIA	secunia.com
Support / Security / Advisories // MDVSA-2011:024 Mandriva	MANDRIVA	www.mandriva.com
Support / Security / Advisories // MDVSA-2011:025 Mandriva	MANDRIVA	www.mandriva.com
KDC denial of service attacks - SecurityReason.com	SREASON	securityreason.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
VMSA-2011-0012.2	CONFIRM	www.vmware.com
Support	REDHAT	www.redhat.com
About Secunia Research Flexera	SECUNIA	secunia.com
web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-002.txt	CONFIRM	web.mit.edu
SecurityFocus	BUGTRAQ	www.securityfocus.com
Kerberos Key Distribution Center (KDC) Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com
Red Hat update for krb5 - Secunia.com	SECUNIA	secunia.com
Webmail - OVH	VUPEN	www.vupen.com
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [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](#) 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](#)