



CVE-2011-0284

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

Summary

CVE	CVE-2011-0284
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-20 02:00:00 UTC
Updated	2020-01-21 15:46:00 UTC
Description	Double free vulnerability in the prepare_error_as function in do_as_req.c in the Key Distribution Center (KDC) in MIT Kerbe

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.7	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
-----------	--------	------

Support	REDHAT	www.redhat.com
Red Hat update for krb5 - Secunia.com	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vulnhub.com
Kerberos KDC "prepare_error_as" Double-Free Vulnerability - Secunia.com	SECUNIA	secunia.com
71183	OSVDB	osvdb.org
SecurityFocus	BUGTRAQ	www.securityfocus.com
web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-003.txt	CONFIRM	web.mit.edu
[SECURITY] Fedora 13 Update: krb5-1.7.1-18.fc13	FEDORA	lists.fedoraproject.org
US-CERT Vulnerability Note VU#943220 - MIT KDC vulnerable to double-free when PKINIT enabled	CERT-VN	www.kb.cert.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vulnhub.com
USN-1088-1: Kerberos vulnerability Ubuntu	UBUNTU	www.ubuntu.com
MIT Kerberos KDC 'do_as_req.c' Double Free Memory Corruption Vulnerability	BID	www.securityfocus.com
Fedora update for krb5 - Secunia.com	SECUNIA	secunia.com
MIT Kerberos KDC Double Free in perpare_error_as() Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	securitytracker.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vulnhub.com
Webmail- OVH	VUPEN	www.vulnhub.com
Support / Security / Advisories / / MDVSA-2011:048 Mandriva	MANDRIVA	www.mandriva.com
[SECURITY] Fedora 15 Update: krb5-1.9-6.fc15	FEDORA	lists.fedoraproject.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	SUSE	lists.opensuse.org
[SECURITY] Fedora 14 Update: krb5-1.8.2-9.fc14	FEDORA	lists.fedoraproject.org
Ubuntu update for krb5 - Advisories - Community	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vulnhub.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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report