



CVE-2007-0957

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

Summary

CVE	CVE-2007-0957
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-06 01:19:00 UTC
Updated	2021-02-02 18:24:00 UTC
Description	Stack-based buffer overflow in the krb5_klog_syslog function in the kadm5 library, as used by the Kerberos administration c

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Application	Mit	Kerberos 5	All	All	All	All

References

Reference	Source
Support	RI
Debian update for krb5 - Advisories - Secunia	SE

US-CERT Technical Cyber Security Alert TA07-109A -- Apple Updates for Multiple Vulnerabilities	CI
Webmail - OVH	VL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
Mandriva update for krb5 - Advisories - Secunia	SE
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: krb5 (SUSE-SA:2007:025)	SU
SGI update for krb5 - Advisories - Secunia	SE
SecurityFocus	BU
APPLE-SA-2007-04-19 Security Update 2007-004	AF
US-CERT Vulnerability Note VU#704024	CI
Red Hat update for krb5 - Advisories - Secunia	SE
Advisories - Mandriva Linux	ML
102930	SU
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
MIT Kerberos 5 KAdminD Server Stack Buffer Overflow Vulnerability	BI
About Security Update 2007-004	CO
Novell Kerberos KDC "krb5_klog_syslog()" Buffer Overflow - Advisories - Secunia	SE
20070401-01-P	SC
Kerberos kadmin/KDC Stack Overflow in krb5_klog_syslog() Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker	SE
SUSE update for krb5 - Advisories - Secunia	SE
rPath updates for krb5 - Advisories - Secunia	SE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VL
Gentoo update for mit-krb5 - Advisories - Secunia	SE
IBM X-Force Exchange	XF
Gentoo Linux Documentation -- MIT Kerberos 5: Arbitrary remote code execution	GL
US-CERT Technical Cyber Security Alert TA07-093B -- MIT Kerberos Vulnerabilities	CI
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	SE
SecurityFocus	BU
SecurityFocus	BU
USN-449-1: krb5 vulnerabilities Ubuntu	UI
Kerberos Multiple Vulnerabilities - Advisories - Secunia	SE
Sun Solaris Kerberos kadm5 Library Vulnerability - Advisories - Secunia	SE
web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-002-syslog.txt	CO
Debian -- Security Information -- DSA-1276-1 krb5	DI
Repository / Oval Repository	O'
Ubuntu update for krb5 - Advisories - Secunia	SE
OVHcloud - Solution de messagerie professionnelle - OVHcloud- OVH	VL

CVE Program record	CVE
NVD vulnerability detail	NVD
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](#)