



CVE-2006-6143

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

Summary

CVE	CVE-2006-6143
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-31 05:00:00 UTC
Updated	2020-01-21 15:45:00 UTC
Description	The RPC library in Kerberos 5 1.4 through 1.4.4, and 1.5 through 1.5.1, as used in Kerberos administration daemon (kadmi

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	1.4	All	All	All
Application	Mit	Kerberos 5	1.4.1	All	All	All
Application	Mit	Kerberos 5	1.4.2	All	All	All
Application	Mit	Kerberos 5	1.4.3	All	All	All
Application	Mit	Kerberos 5	1.4.4	All	All	All
Application	Mit	Kerberos 5	1.5	All	All	All
Application	Mit	Kerberos 5	1.5.1	All	All	All
Application	Mit	Kerberos 5	1.4	All	All	All
Application	Mit	Kerberos 5	1.4.1	All	All	All
Application	Mit	Kerberos 5	1.4.2	All	All	All
Application	Mit	Kerberos 5	1.4.3	All	All	All
Application	Mit	Kerberos 5	1.4.4	All	All	All
Application	Mit	Kerberos 5	1.5	All	All	All
Application	Mit	Kerberos 5	1.5.1	All	All	All

References

Reference	Source
-----------	--------

404 Not Found	FED
Webmail - OVH	VUL
OpenPKG Corporation: Security: Security Advisories	OP
Fedora Core 6 update for krb5 - Advisories - Secunia	SEC
US-CERT Technical Cyber Security Alert TA07-109A -- Apple Updates for Multiple Vulnerabilities	CEI
Webmail - OVH	VUL
Mandriva update for krb5 - Advisories - Secunia	SEC
SecurityFocus	BU
Ubuntu update for krb5 - Advisories - Secunia	SEC
Gentoo Linux Documentation -- MIT Kerberos 5: Arbitrary Remote Code Execution	GE
APPLE-SA-2007-04-19 Security Update 2007-004	API
USN-408-1: krb5 vulnerability Ubuntu	UBI
web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2006-002-rpc.txt	CO
Kerberos kadmind xpirt->xp_auth Code Execution Vulnerability - Advisories - Secunia	SEC
About Security Update 2007-004	CO
[SECURITY] Fedora Core 6 Update: krb5-1.5-13 FedoraNEWS.ORG	FED
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: krb5 security problems (SUSE-SA:2007:004)	SU
Fedora Core 5 update for krb5 - Advisories - Secunia	SEC
Kerberos kadmind SVCAUTH_DESTROY() Lets Remote Users Execute Arbitrary Code - SecurityTracker	SEC
issues.rpath.com/browse/RPL-925	CO
Advisories Mandriva	MA
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	SEC
US-CERT Vulnerability Note VU#481564	CEI
Gentoo update for mit-krb5 - Advisories - Secunia	SEC
MIT Kerberos 5 RPC Library Remote Code Execution Vulnerability	BID
US-CERT Technical Cyber Security Alert TA07-009B -- MIT Kerberos Vulnerabilities	CEI
31281	OS
IBM X-Force Exchange	XF
SUSE update for Kerberos - Advisories - Secunia	SEC
CVE Program record	CVI
NVD vulnerability detail	NVI
◀ ▶	

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Not vulnerable. Red Hat Enterprise Linux 2.1, 3, and 4 ship with versions of Kerberos 5 prior to v
◀ ▶			

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](#)