



CVE-2014-5353

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

Summary

CVE	CVE-2014-5353
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-16 23:59:00 UTC
Updated	2021-02-02 18:57:00 UTC
Description	The krb5_ldap_get_password_policy_from_dn function in plugins/kdb/ldap/libkdb_ldap/ldap_pwd_policy.c in MIT Kerberos

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All

Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References		
Reference	Source	Link
#773226 - CVE-2014-5353: misused policy name crashes KDC - Debian Bug report logs	CONFIRM	bugs.debian.c
USN-2498-1: Kerberos vulnerabilities Ubuntu	UBUNTU	www.ubuntu.c
Fix LDAP misused policy name crash [CVE-2014-5353] · krb5/krb5@d1f7070 · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	rhn.redhat.co
[SECURITY] Fedora 22 Update: krb5-1.13.1-2.fc22	FEDORA	lists.fedorapro
[SECURITY] [DLA 1265-1] krb5 security update	MLIST	lists.debian.or
Mageia Advisory: MGASA-2014-0536 - Updated krb5 packages fix CVE-2014-5353	CONFIRM	advisories.ma
MIT Kerberos Null Pointer Dereference Bugs Let Remote Authenticated Users Deny Service - SecurityTracker	SECTrack	www.securityt
openSUSE-SU-2015:0542-1: moderate: Security update for krb5	SUSE	lists.opensuse
Red Hat Customer Portal	REDHAT	rhn.redhat.co
Support / Security / Advisories // MDVSA-2015:009 Mandriva	MANDRIVA	www.mandriva
MIT Kerberos 5 CVE-2014-5353 NULL Pointer Dereference Remote Denial of Service Vulnerability	BID	www.securityt
Oracle Solaris Third Party Bulletin - April 2015	CONFIRM	www.oracle.c
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.

[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