CVE-2014-4345

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-4345
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-14 05:01:50 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Off-by-one error in the krb5_encode_krbsecretkey function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KI

Risk And Classification

Primary CVSS: v2.0 8.5 from nvd@nist.gov

AV:N/AC:M/Au:S/C:C/I:C/A:C

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos 5	1.10	All	All	All

Application	Mit	Kerberos 5	1.10.1	All	All	All
Application	Mit	Kerberos 5	1.10.2	All	All	All
Application	Mit	Kerberos 5	1.10.3	All	All	All
Application	Mit	Kerberos 5	1.10.4	All	All	All
Application	Mit	Kerberos 5	1.11	All	All	All
Application	Mit	Kerberos 5	1.11.1	All	All	All
Application	Mit	Kerberos 5	1.11.2	All	All	All
Application	Mit	Kerberos 5	1.11.3	All	All	All
Application	Mit	Kerberos 5	1.11.4	All	All	All
Application	Mit	Kerberos 5	1.11.5	All	All	All
Application	Mit	Kerberos 5	1.12	All	All	All
Application	Mit	Kerberos 5	1.12.1	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	1.8.4	All	All	All
Application	Mit	Kerberos 5	1.8.5	All	All	All
Application	Mit	Kerberos 5	1.8.6	All	All	All
Application	Mit	Kerberos 5	1.9	All	All	All
Application	Mit	Kerberos 5	1.9.1	All	All	All
Application	Mit	Kerberos 5	1.9.2	All	All	All
Application	Mit	Kerberos 5	1.9.3	All	All	All
Application	Mit	Kerberos 5	1.9.4	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Debian -- Security Information -- DSA-2000-1 krb5

Debian -- Security Information -- DSA-3000-1 krb5
Fix +1 error in storing krbPrincipalKey LDAP attr. by tkuthan · Pull Request #181 · krb5/krb5 · GitHub
IBM X-Force Exchange
About Secunia Research | Flexera
Security Advisory SA59415 - Oracle Solaris Kerberos kadmind LDAP Backend Buffer Overflow Vulnerability - Secunia
Security Advisory SA61353 - Red Hat update for krb5 - Secunia
Security Advisory SA61314 - Oracle Linux update for krb5 - Secunia
[security-announce] SUSE-SU-2014:1028-1: important: Security update for
MIT kerberos 5 'ldap_principal2.c' Buffer Overflow Vulnerability
Security Advisory SA59102 - Debian update for krb5 - Secunia
Mageia Advisory: MGASA-2014-0345 - Updated krb5 package fixes security vulnerabilities
MIT Kerberos 5: User-assisted execution of arbitrary code (GLSA 201412-53) — Gentoo security
openSUSE-SU-2014:1043-1: moderate: update for krb5, krb5-doc, krb5-mini
RT/krbdev.mit.edu: Ticket #7980 LDAP key data segmentation buffer overflow [CVE-2014-4345]
www.osvdb.org/109908
Oracle Critical Patch Update - October 2017
CVE-2014-4345 Numeric Errors vulnerability in Kerberos (Third Party Vulnerability Resolution Blog)
Security Advisory SA60776 - SUSE update for krb5 - Secunia
Red Hat Customer Portal
linux.oracle.com | ELSA-2014-1255
MIT Kerberos Buffer Overflow in kadmind with LDAP Backend Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker
About Secunia Research | Flexera
Fix LDAP key data segmentation [CVE-2014-4345] · krb5/krb5@dc7ed55 · GitHub
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView
1128157 – (CVE-2014-4345) CVE-2014-4345 krb5: buffer overrun in kadmind with LDAP backend (MITKRB5-SA-2014-001)
mandriva.com
Red Hat Customer Portal
web.mit.edu/kerberos/advisories/MITKRB5-SA-2014-001.txt
[SECURITY] Fedora 20 Update: krb5-1.11.5-11.fc20
[SECURITY] Fedora 19 Update: krb5-1.11.3-25.fc19
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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