CVE-2008-0947

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

Summary

CVE	CVE-2008-0947
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-19 00:44:00 UTC
Updated	2020-01-21 15:45:00 UTC
Description	Buffer overflow in the RPC library used by libgssrpc and kadmind in MIT Kerberos 5 (krb5) 1.4 through 1.6.3 allows remote

Risk And Classification

Problem Types: CWE-119

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	1.5.2	All	All	All
Application	Mit	Kerberos 5	1.5.3	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	1.6.3	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
Application	Mit	Kerberos 5	1.5.2	All	All	All
Application	Mit	Kerberos 5	1.5.3	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	1.6.3	All	All	All

References

Reference	Source	Link
novell-kerberos 20080331	CONFIRM	supp
Advisories:rPSA-2008-0112 - rPath Wiki	CONFIRM	wiki.
Repository / Oval Repository	OVAL	oval
Debian update for krb5 - Advisories - Secunia	SECUNIA	secu
US-CERT Technical Cyber Security Alert TA08-079B -- MIT Kerberos Updates for Multiple Vulnerabilities	CERT	www
rPath update for krb5 - Advisories - Secunia	SECUNIA	secu
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www
Support | Red Hat	REDHAT	www
Fedora update for krb5 - Advisories - Secunia	SECUNIA	secu
Kerberos Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secu
IBM X-Force Exchange	XF	exch
Gentoo update for krb5 - Advisories - Secunia	SECUNIA	secu
USN-587-1: Kerberos vulnerabilities | Ubuntu	UBUNTU	www
web.mit.edu/kerberos/advisories/MITKRB5-SA-2008-002.txt	CONFIRM	web
[SECURITY] Fedora 7 Update: krb5-1.6.1-9.fc7	FEDORA	www
SecurityFocus	BUGTRAQ	www
US-CERT Vulnerability Notes	CERT-VN	www
SecurityFocus	BUGTRAQ	www
MIT Kerberos 5: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	secu
Advisories:rPSA-2008-0112 - rPath Wiki	CONFIRM	wiki.
SecurityReason - double-free, uninitialized data vulnerabilities in krb5kdc	SREASON	secu
Red Hat update for krb5 - Advisories - Secunia	SECUNIA	secu
Mandriva update for krb5 - Advisories - Secunia	SECUNIA	secu

novell-kerberos 20080331	CONFIRM	supp
[SECURITY] Fedora 8 Update: krb5-1.6.2-14.fc8	FEDORA	www
Novell Kerberos KDC Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secu
MIT Kerberos5 kadmind Excessive File Descriptors Multiple Remote Code Execution Vulnerabilities	BID	www
Debian -- Security Information -- DSA-1524-1 krb5	DEBIAN	www
Kerberos kadmind RPC Library Array Overrun May Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www
Advisories | Mandriva	MANDRIVA	www
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www
Ubuntu update for krb5 - Advisories - Secunia	SECUNIA	secu
SecurityFocus	BUGTRAQ	www
Advisories | Mandriva	MANDRIVA	www
SUSE update for krb5 - Advisories - Secunia	SECUNIA	secu
'[security bulletin] HPSBOV02682 SSRT100495 rev.1 - HP OpenVMS running Kerberos, Remote Denial of Ser' - MARC	HP	mar
[security-announce] SUSE Security Announcement: krb5 (SUSE-SA:2008:016)	SUSE	lists
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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