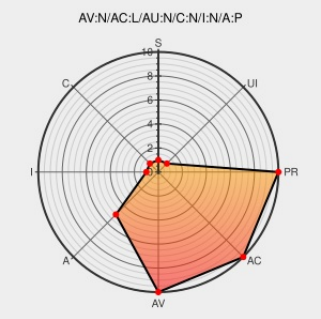
CVE-2005-1174

Published on: 07/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1174

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Kerberos 5 from Mit contain the following vulnerability:

MIT Kerberos 5 (krb5) 1.3 through 1.4.1 Key Distribution Center (KDC) allows remote attackers to cause a denial of service (application crash) via a certain valid TCP connection that causes a free of unallocated memory.

CVE-2005-1174 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
#101809: Security Vulnerabilities in the Kerberos Key Distribution Center (KDC) Daemon	web.archive.org, text/html, Inactive Link, Not Archived	SUNALERT 101809
404 Not Found	www.turbolinux.com, text/plain, Inactive Link, Not Archived	TURBO TLSA-2005-78
IBM notice: The page you requested cannot be displayed	www-1.ibm.com, text/html, Inactive Link, Not Archived	AIXAPAR IY85474
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com, text/html	VUPEN ADV-2006-2074
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:10229

Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:017
Support	www.redhat.com text/html	REDHAT RHSA-2005:567
	Patch web.mit.edu text/plain	CONFIRM web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20050703-01-U
Secunia - Advisories - Kerberos V5 Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16041
USN-224-1: Kerberos vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-224-1
Secunia - Advisories - Ubuntu update for kerberos	web.archive.org text/html	SECUNIA 17899
SecurityTracker.com Archives - MIT krb5 KDC Buffer Overflow in 'do_as_req' and 'do_tgs_req' May Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1014460
Secunia - Advisories - IBM DCE Two Kerberos Vulnerabilities	web.archive.org text/html	SECUNIA 20364
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2005-0036
Debian -- Security Information -- DSA-757-1 krb5	www.debian.org Depreciated Link text/html	DEBIAN DSA-757
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF kerberos-kdc-krb5-tcp-connection-dos(21327)
'MITKRB5-SA-2005-002: buffer overflow, heap corruption in KDC' - MARC	marc.info text/html	BUGTRAQ 20050712 MITKRB5-SA-2005-002: buffer overflow, heap corruption in KDC
MIT Kerberos 5 Key Distribution Center Remote Denial of Service Vulnerability	cve.report (archive) text/html	BID 14240
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:397
APPLE-SA-2005-08-17 Security Update 2005-007 v1.1	lists.apple.com text/html	APPLE APPLE-SA-2005-08-17
APPLE-SA-2005-08-15 Security Update 2005-007	lists.apple.com text/html	APPLE APPLE-SA-2005-08-15
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com inode/x-empty	VUPEN ADV-2005-1066
US-CERT Vulnerability Note VU#259798	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#259798

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos 5	1.3	All	All	All
Application	Mit	Kerberos 5	1.3.1	All	All	All
Application	Mit	Kerberos 5	1.3.2	All	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Mit	Kerberos 5	1.3.4	All	All	All
Application	Mit	Kerberos 5	1.3.5	All	All	All
Application	Mit	Kerberos 5	1.3.6	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	1.3	All	All	All
Application	Mit	Kerberos 5	1.3.1	All	All	All
Application	Mit	Kerberos 5	1.3.2	All	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Mit	Kerberos 5	1.3.4	All	All	All
Application	Mit	Kerberos 5	1.3.5	All	All	All
Application	Mit	Kerberos 5	1.3.6	All	All	All
Application	Mit	Kerberos 5	1.4	All	All	All
Application	Mit	Kerberos 5	1.4.1	All	All	All

cpe:2.3:a:mit:kerberos_5:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→