



CVE-2001-0035

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

Summary

CVE	CVE-2001-0035
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-02-16 05:00:00 UTC
Updated	2017-10-10 01:29:00 UTC
Description	Buffer overflow in the kdc_reply_cipher function in KTH Kerberos IV allows remote attackers to cause a denial of service an

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kth	Kth Kerberos	4	All	All	All
Application	Kth	Kth Kerberos	4	All	All	All

References

Reference	Source	Li
Neohapsis Archives - Bugtraq - KTH upgrade and FIX - From vipi@FASTFLOWSRL.COM	BUGTRAQ	ar
Neohapsis Archives - Bugtraq - Buffer overflow in old ssh-1.2.2x-afs-kerberosv4 patches - From dugsong@MONKEY.ORG	BUGTRAQ	ar
Neohapsis Archives - Bugtraq - Vulnerabilities in KTH Kerberos IV - From jouko@SOLUTIONS.FI	BUGTRAQ	ar
IBM X-Force Exchange	XF	ex
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)