



CVE-2005-0468

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2005-0468
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Heap-based buffer overflow in the env_opt_add function in telnet.c for various BSD-based Telnet clients allows remote atta

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ncsa	Telnet	c	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
US-CERT Vulnerability Note VU#341908			af854a3a-2127-422b-9	
rhn.redhat.com Red Hat Support			af854a3a-2127-422b-9	
patches.sgi.com/support/free/security/advisories/20050405-01-P			af854a3a-2127-422b-9	
Secunia - Advisories - MIT Kerberos Telnet Client Buffer Overflow Vulnerabilities			af854a3a-2127-422b-9	
Debian -- Security Information -- DSA-731-1 krb4			af854a3a-2127-422b-9	
Advisories - Mandriva			af854a3a-2127-422b-9	
Debian -- Security Information -- DSA-703-1 krb5			af854a3a-2127-422b-9	
rhn.redhat.com Red Hat Support			af854a3a-2127-422b-9	
Multiple Vendor Telnet Client Env_opt_add Heap-Based Buffer Overflow Vulnerability			af854a3a-2127-422b-9	
Home - Conectiva			af854a3a-2127-422b-9	
#101671: Buffer Overflow in telnet(1) Client Software Also Affects Kerberized Telnet (formerly Document ID: 57761)			af854a3a-2127-422b-9	
#101665: Buffer Overflow in telnet(1) Client Software (formerly Document ID: 57755)			af854a3a-2127-422b-9	
ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:01.telnet.asc			af854a3a-2127-422b-9	
#101665: Buffer Overflow in telnet(1) Client Software (formerly Document ID: 57755)			af854a3a-2127-422b-9	
#101671: Buffer Overflow in telnet(1) Client Software Also Affects Kerberized Telnet (formerly Document ID: 57761)			af854a3a-2127-422b-9	
Repository / Oval Repository			af854a3a-2127-422b-9	
Accenture Let there be change			af854a3a-2127-422b-9	
USN-224-1: Kerberos vulnerabilities Ubuntu security notices Ubuntu			af854a3a-2127-422b-9	
Secunia - Advisories - Ubuntu update for kerberos			af854a3a-2127-422b-9	
web.mit.edu/kerberos/advisories/MITKRB5-SA-2005-001-telnet.txt			af854a3a-2127-422b-9	
CVE Program record			CVE.ORG	
NVD vulnerability detail			NVD	
Vendor Comments And Credit				
Organization	Published	Contributor	Statement	
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.	
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](#).

Free CVE JSON API [cve.report/api](#)

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