



# CVE-2011-4862

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

## Summary

<b>CVE</b>	CVE-2011-4862
<b>State</b>	PUBLIC
<b>Assigner</b>	secteam@freebsd.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-12-25 01:55:00 UTC
<b>Updated</b>	2021-02-09 14:48:00 UTC
<b>Description</b>	Buffer overflow in libtelnet/encrypt.c in telnetd in FreeBSD 7.3 through 9.0, MIT Kerberos Version 5 Applications (aka krb5-...

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	5.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	6.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	5.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	6.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	15	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	16	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	15	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	16	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Inetutils</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Inetutils</a>	All	All	All	All
Application	<a href="#">Heimdal Project</a>	<a href="#">Heimdal</a>	All	All	All	All
Application	<a href="#">Mit</a>	<a href="#">Krb5-appl</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	10	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	10	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	10	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	10	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	10	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	9	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	10	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	10	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	10	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	9	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	10	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	11	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	10	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	11	sp1	All	All

## References

Reference	Source	Link
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.com</a>
Support	REDHAT	<a href="#">www.redhat.com</a>
Support	REDHAT	<a href="#">www.redhat.com</a>
[SECURITY] Fedora 16 Update: krb5-appl-1.0.2-2.fc16	FEDORA	<a href="#">lists.fedoraproject.org</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.com</a>
Support	REDHAT	<a href="#">www.redhat.com</a>
Debian -- Security Information -- DSA-2372-1 heimdal	DEBIAN	<a href="#">www.debian.org</a>
FreeBSD-SA-11:08	FREEBSD	<a href="#">security.freebsd.org</a>
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>
Support / Security / Advisories // MDVSA-2011:195   Mandriva	MANDRIVA	<a href="#">www.mandriva.com</a>
Microsoft Security Bulletin MS11-051	SECUNIA	<a href="#">secunia.com</a>

About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
Merry Christmas from the FreeBSD Security Team	MLIST	<a href="#">lists.freeb</a>
<a href="#">web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2011-008.txt</a>	CONFIRM	<a href="#">web.mit.e</a>
Telnetd encrypt_keyid: Remote Root function pointer overwrite	EXPLOIT-DB	<a href="#">www.exp</a>
<a href="#">security.freebsd.org/patches/SA-11:08/telnetd.patch</a>	CONFIRM	<a href="#">security.f</a>
[security-announce] SUSE-SU-2012:0050-1: important: Security update for	SUSE	<a href="#">lists.oper</a>
inetutils.git - GNU Inetutils	CONFIRM	<a href="#">git.savan</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
Merry Christmas from the FreeBSD Security Team	MLIST	<a href="#">lists.freeb</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
FreeBSD Telnet Encryption Feature Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">www.sec</a>
[security-announce] SUSE-SU-2012:0010-1: important: Security update for	SUSE	<a href="#">lists.oper</a>
[security-announce] SUSE-SU-2012:0042-1: important: Security update for	SUSE	<a href="#">lists.oper</a>
Debian -- Security Information -- DSA-2375-1 krb5, krb5-appl	DEBIAN	<a href="#">www.dek</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
Merry Christmas from the FreeBSD Security Team	MLIST	<a href="#">lists.freeb</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
[SECURITY] Fedora 15 Update: krb5-appl-1.0.1-8.fc15	FEDORA	<a href="#">lists.fedo</a>
[security-announce] SUSE-SU-2012:0056-1: important: Security update for	SUSE	<a href="#">lists.oper</a>
Merry Christmas from the FreeBSD Security Team	MLIST	<a href="#">lists.freeb</a>
78020	OSVDB	<a href="#">osvdb.or</a>
[security-announce] openSUSE-SU-2012:0019-1: important: krb5-appl: Fixed	SUSE	<a href="#">lists.oper</a>
[security-announce] SUSE-SU-2012:0024-1: important: Security update for	SUSE	<a href="#">lists.oper</a>
Kerberos Telnet Encryption Feature Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">www.sec</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
Debian -- Security Information -- DSA-2373-1 inetutils	DEBIAN	<a href="#">www.dek</a>
Support	REDHAT	<a href="#">www.red</a>
About Secunia Research   Flexera	SECUNIA	<a href="#">secunia.c</a>
NEOHAPSIS - Peace of Mind Through Integrity and Insight	BUGTRAQ	<a href="#">archives.</a>
[security-announce] SUSE-SU-2012:0018-1: important: Security update for	SUSE	<a href="#">lists.oper</a>
[security-announce] openSUSE-SU-2012:0051-1: important: krb5-appl: Fixed	SUSE	<a href="#">lists.oper</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

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](#)