



# CVE-2011-1526

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

## Summary

<b>CVE</b>	CVE-2011-1526
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-07-11 20:55:00 UTC
<b>Updated</b>	2021-02-02 18:36:00 UTC
<b>Description</b>	ftpd.c in the GSS-API FTP daemon in MIT Kerberos Version 5 Applications (aka krb5-appl) 1.0.1 and earlier does not check

## Risk And Classification

**Problem Types:** CWE-269

## 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>	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="#">Fedoraproject</a>	<a href="#">Fedora</a>	14	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>	14	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	15	All	All	All
Application	<a href="#">Mit</a>	<a href="#">Krb5-appl</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>	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 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
Support / Security / Advisories // MDVSA-2011:117   Mandriva	MANDRIVA
Support	REDHAT
Debian -- Security Information -- DSA-2283-1 krb5-appl	DEBIAN
web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-005.txt	CONFIRM
73617	OSVDB
MIT Kerberos krb5-appl FTP Daemon EGID Remote Privilege Escalation Vulnerability	BID
SecurityFocus	BUGTRAQ
IBM X-Force Exchange	XF
Security Advisory SA48101 - Red Hat update for krb5 - Secunia	SECUNIA
[security-announce] openSUSE-SU-2011:1169-1: important: krb5: fixed kdc	SUSE
[security-announce] SUSE-SU-2012:0050-1: important: Security update for	SUSE
711419 – (CVE-2011-1526) CVE-2011-1526 krb5, krb5-appl: ftpd incorrect group privilege dropping (MITKRB5-SA-2011-005)	CONFIRM
FTP daemon fails to set effective group ID - CXSecurity.com	SREASON
[security-announce] SUSE-SU-2012:0010-1: important: Security update for	SUSE
Red Hat update for krb5-appl - Secunia.com	SECUNIA
[security-announce] SUSE-SU-2012:0042-1: important: Security update for	SUSE
[SECURITY] Fedora 14 Update: krb5-appl-1.0.1-4.fc14	FEDORA
[SECURITY] Fedora 15 Update: krb5-appl-1.0.1-4.fc15	FEDORA

[SECURITY] Fedora 15 Update: krb5-appl-1.0.1-7.fc15	FEDORA
[security-announce] openSUSE-SU-2012:0019-1: important: krb5-appl: Fixed	SUSE
Kerberos Applications GSS-API FTP Daemon Effective Group ID Privileges Security Issue - Secunia.com	SECUNIA
[security-announce] SUSE-SU-2012:0018-1: important: Security update for	SUSE
[security-announce] openSUSE-SU-2012:0051-1: important: krb5-appl: Fixed	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)**