



CVE-2010-3074

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

Summary

CVE	CVE-2010-3074
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-17 18:00:00 UTC
Updated	2011-01-14 06:46:00 UTC
Description	SSL_Cipher.cpp in EncFS before 1.7.0 uses an improper combination of an AES cipher and a CBC cipher mode for encrypt

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arg0	Encfs	1.4.0	All	All	All
Application	Arg0	Encfs	1.4.1	All	All	All
Application	Arg0	Encfs	1.4.1.1	All	All	All
Application	Arg0	Encfs	1.4.2	All	All	All
Application	Arg0	Encfs	1.5.0	All	All	All
Application	Arg0	Encfs	1.4.0	All	All	All
Application	Arg0	Encfs	1.4.1	All	All	All
Application	Arg0	Encfs	1.4.1.1	All	All	All
Application	Arg0	Encfs	1.4.2	All	All	All
Application	Arg0	Encfs	1.5.0	All	All	All
Application	Arg0	Encfs	All	All	All	All

References

Reference	Source	Link
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:023	SUSE	lists.opensuse.org
oss-security - Re: CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS	MLIST	www.openwall.com
Bug 630460 – CVE-2010-3073 CVE-2010-3074 CVE-2010-3075 fuse-encfs: EncFS: Multiple flaws	CONFIRM	bugzilla.redhat.com

oss-security - CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS	MLIST	www.openwall.com
335938 -- <sys-fs/encfs-1.7.1: Watermarking attack	CONFIRM	bugs.gentoo.org
oss-security - Re: CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS	MLIST	www.openwall.com
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FULLDISC	archives.neohapsis.com
encfs - www	CONFIRM	www.arg0.net
r59 - encfs - Encrypted Filesystem for FUSE - Google Project Hosting	CONFIRM	code.google.com
[SECURITY] Fedora 14 Update: fuse-encfs-1.7.2-1.fc14	FEDORA	lists.fedoraproject.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Fedora update for fuse-encfs - Advisories - Community	SECUNIA	secunia.com
EncFS Multiple Weaknesses - Advisories - Community	SECUNIA	secunia.com
[SECURITY] Fedora 12 Update: fuse-encfs-1.7.2-1.fc12	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 13 Update: fuse-encfs-1.7.2-1.fc13	FEDORA	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://the-mitre-corporation.com) and the authoritative source of CVE content is [MITRE's CVE web site](http://mitre.org/cve). This site includes MITRE data granted under the following [license](http://mitre.org/cve).

CVE.report and Source URL Uptime Status status.cve.report