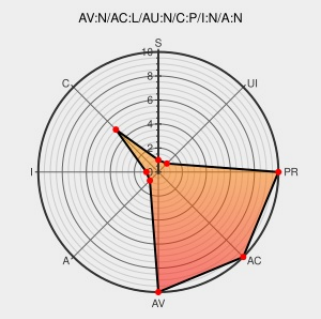
CVE-2010-3075

Published on: 09/17/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:06 AM UTC

CVE-2010-3075

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Encfs from Arg0 contain the following vulnerability:

EncFS before 1.7.0 encrypts multiple blocks by means of the CFB cipher mode with the same initialization vector, which makes it easier for local users to obtain sensitive information via calculations involving recovery of XORed data, as demonstrated by an attack on encrypted data in which the last block contains only one byte.

CVE-2010-3075 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
oss-security - Re: CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS	www.openwall.com text/html	MLIST [oss-security] 20100905 Re: CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS
Bug 630460 – CVE-2010-3073 CVE-2010-3074 CVE-2010-3075 fuse-encfs: EncFS: Multiple flaws	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=630460
oss-security - CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS	www.openwall.com text/html	MLIST [oss-security] 20100905 CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS
oss-security - Re: CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS	www.openwall.com text/html	MLIST [oss-security] 20100907 Re: CVE Request -- EncFS / fuse-encfs [three ids] -- Multiple Vulnerabilities in EncFS
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html	FULLDISC 20100826 Multiple Vulnerabilities in EncFS

	Inactive Link Not Archived	
encfs - www	www.arg0.net text/html	CONFIRM www.arg0.net/encfs
[SECURITY] Fedora 14 Update: fuse-encfs-1.7.2-1.fc14	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-14200
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-2414
Fedora update for fuse-encfs - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 41478
EncFS Multiple Weaknesses - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 41158
[SECURITY] Fedora 12 Update: fuse-encfs-1.7.2-1.fc12	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-14254
[SECURITY] Fedora 13 Update: fuse-encfs-1.7.2-1.fc13	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-14268

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:arg0:encfs:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:arg0:encfs:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→