



# CVE-2009-1574

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

## Summary

<b>CVE</b>	CVE-2009-1574
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-05-06 17:30:00 UTC
<b>Updated</b>	2017-09-29 01:34:00 UTC
<b>Description</b>	racoon/isakmp_frag.c in ipsec-tools before 0.7.2 allows remote attackers to cause a denial of service (crash) via crafted frag

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.1	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.2	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.2.1	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.2.2	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.2.3	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.2.4	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3	rc1	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3	rc2	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3	rc3	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3	rc4	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3	rc5	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3.1	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3.2	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.3.3	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.4	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.4	rc1	All	All

Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.5	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.1	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.2	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.3	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.4	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.5	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.6	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.7	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	All	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.1	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.2	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.2.1	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.2.2	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.2.3	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.2.4	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3	rc1	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3	rc2	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3	rc3	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3	rc4	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3	rc5	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3.1	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3.2	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.3.3	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.4	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.4	rc1	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.5	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.1	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.2	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.3	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.4	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.5	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.6.6	All	All	All
Application	<a href="#">Ipsec-tools</a>	<a href="#">Ipsec-tools</a>	0.7	All	All	All

## References

Reference	Source	Link
About Security Update 2009-006 / Mac OS X v10.6.2	CONFIRM	<a href="http://support.apple.com">support.apple.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.it">exchange.xforce.it</a>
IPsec-Tools Prior to 0.7.2 Multiple Remote Denial Of Service Vulnerabilities	BID	<a href="http://www.securityfocus">www.securityfocus</a>
About the security content of Time Capsule and AirPort Base Station (802.11n) Firmware 7.5.2	CONFIRM	<a href="http://support.apple.com">support.apple.com</a>
APPLE-SA-2009-11-09-1 Security Update 2009-006 / Mac OS X v10.6.2	APPLE	<a href="http://lists.apple.com">lists.apple.com</a>
Red Hat update for ipsec-tools - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[SECURITY] Fedora 11 Update: ipsec-tools-0.7.2-1.fc11	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>
497990 – (CVE-2009-1574) CVE-2009-1574 ipsec-tools: racoon NULL dereference in fragmentation code	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
Debian update for ipsec-tools - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Gentoo update for ipsec-tools - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
oss-security - ipsec-tools 0.7.2	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
[SECURITY] Fedora 9 Update: ipsec-tools-0.7.2-1.fc9	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
APPLE-SA-2010-12-16-1 Time Capsule and AirPort Base Station (802.11n) Firmware 7.5.2	APPLE	<a href="http://lists.apple.com">lists.apple.com</a>
USN-785-1: ipsec-tools vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:012	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
Support / Security / Advisories // MDVSA-2009:112   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Debian -- Security Information -- DSA-1804-1 ipsec-tools	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Ubuntu update for ipsec-tools - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Fedora update for ipsec-tools - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Gentoo Linux Documentation -- IPSec Tools: Denial of Service	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
[PROJECT ABANDONED] IPsec Tools download   SourceForge.net	CONFIRM	<a href="http://sourceforge.net">sourceforge.net</a>
[SECURITY] Fedora 10 Update: ipsec-tools-0.7.2-1.fc10	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
oss-security - Re: ipsec-tools 0.7.2	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	CONFIRM	<a href="http://kb.juniper.net">kb.juniper.net</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](#)**