



# CVE-2005-3732

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

## Summary

<b>CVE</b>	CVE-2005-3732
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-11-21 22:03:00 UTC
<b>Updated</b>	2018-10-19 15:38:00 UTC
<b>Description</b>	The Internet Key Exchange version 1 (IKEv1) implementation (isakmp_agg.c) in racoon in ipsec-tools before 0.6.3, when ru

## Risk And Classification

**Problem Types:** CWE-399

## 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>	0.5	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.5.1	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.5.2	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.6	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>	0.5	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.5.1	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.5.2	All	All	All
Application	<a href="#">ipsec-tools</a>	<a href="#">ipsec-tools</a>	0.6	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

## References

### Reference

[www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp](http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp)

[rhn.redhat.com](http://rhn.redhat.com) | Red Hat Support

SecurityFocus
Secunia - Advisories - Debian update for ipsec-tools
SourceForge.net: BlackBerryTools: blackberrytools-users
USN-221-1: racoon vulnerability   Ubuntu security notices
Secunia - Advisories - SUSE update for ipsec-tools / freeswan / openswan
Debian -- Security Information -- DSA-965-1 ipsec-tools
Neohapsis Archives - Bugtraq - #0161 - Re: [ GLSA 200512-04 ] Openswan, IPsec-Tools: Vulnerabilities in ISAK MP Protocol implementation
20060501-01-U
SecurityTracker.com Archives - IPSec-tools IKE Processing Lets Remote Users Deny Service
Security Announcement
Repository / Oval Repository
Secunia - Advisories - Ubuntu update for ipsec-tools
Gentoo Linux Documentation -- Openswan, IPsec-Tools: Vulnerabilities in ISAKMP Protocol implementation
cvs.sourceforge.net/viewcvs.py/ipsec-tools/ipsec-tools/src/racoon/isakmp_agg.c
Secunia - Advisories - Red Hat update for ipsec-tools
Secunia - Advisories - IPsec-Tools ISAKMP IKE Message Processing Denial of Service
Secunia - Advisories - Mandriva update for ipsec-tools
www.niscc.gov.uk/niscc/docs/re-20051114-01014.pdf
Advisories - Mandriva Linux
Secunia - Advisories - Gentoo update for openswan / ipsec-tools
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates
IPSec-Tools IKE Message Handling Denial of Service Vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CVE Program record
NVD vulnerability detail

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](#).

