



CVE-2009-1957

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

Summary

CVE	CVE-2009-1957
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-08 01:00:00 UTC
Updated	2009-10-14 05:24:00 UTC
Description	charon/sa/ike_sa.c in the charon daemon in strongSWAN before 4.3.1 allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strongswan	Strongswan	2.0.0	All	All	All
Application	Strongswan	Strongswan	2.0.1	All	All	All
Application	Strongswan	Strongswan	2.0.2	All	All	All
Application	Strongswan	Strongswan	2.1.0	All	All	All
Application	Strongswan	Strongswan	2.1.1	All	All	All
Application	Strongswan	Strongswan	2.1.2	All	All	All
Application	Strongswan	Strongswan	2.1.3	All	All	All
Application	Strongswan	Strongswan	2.1.4	All	All	All
Application	Strongswan	Strongswan	2.1.5	All	All	All
Application	Strongswan	Strongswan	2.2.0	All	All	All
Application	Strongswan	Strongswan	2.2.1	All	All	All
Application	Strongswan	Strongswan	2.2.2	All	All	All
Application	Strongswan	Strongswan	2.3.0	All	All	All
Application	Strongswan	Strongswan	2.3.1	All	All	All
Application	Strongswan	Strongswan	2.3.2	All	All	All
Application	Strongswan	Strongswan	2.4.0	All	All	All
Application	Strongswan	Strongswan	2.4.0a	All	All	All

Application	Strongswan	Strongswan	2.4.1	All	All	All
Application	Strongswan	Strongswan	2.4.2	All	All	All
Application	Strongswan	Strongswan	2.4.3	All	All	All
Application	Strongswan	Strongswan	2.4.4	All	All	All
Application	Strongswan	Strongswan	2.5.0	All	All	All
Application	Strongswan	Strongswan	2.5.1	All	All	All
Application	Strongswan	Strongswan	2.5.2	All	All	All
Application	Strongswan	Strongswan	2.5.3	All	All	All
Application	Strongswan	Strongswan	2.5.4	All	All	All
Application	Strongswan	Strongswan	2.5.5	All	All	All
Application	Strongswan	Strongswan	2.5.6	All	All	All
Application	Strongswan	Strongswan	2.5.7	All	All	All
Application	Strongswan	Strongswan	2.6.0	All	All	All
Application	Strongswan	Strongswan	2.6.1	All	All	All
Application	Strongswan	Strongswan	2.6.16	All	All	All
Application	Strongswan	Strongswan	2.6.2	All	All	All
Application	Strongswan	Strongswan	2.6.20	All	All	All
Application	Strongswan	Strongswan	2.6.3	All	All	All
Application	Strongswan	Strongswan	2.6.4	All	All	All
Application	Strongswan	Strongswan	2.7.0	All	All	All
Application	Strongswan	Strongswan	2.8.0	All	All	All
Application	Strongswan	Strongswan	2.8.1	All	All	All
Application	Strongswan	Strongswan	2.8.2	All	All	All
Application	Strongswan	Strongswan	2.8.3	All	All	All
Application	Strongswan	Strongswan	2.8.4	All	All	All
Application	Strongswan	Strongswan	2.8.5	All	All	All
Application	Strongswan	Strongswan	2.8.6	All	All	All
Application	Strongswan	Strongswan	2.8.7	All	All	All
Application	Strongswan	Strongswan	2.8.8	All	All	All
Application	Strongswan	Strongswan	4.0.0	All	All	All
Application	Strongswan	Strongswan	4.0.1	All	All	All
Application	Strongswan	Strongswan	4.0.2	All	All	All
Application	Strongswan	Strongswan	4.0.3	All	All	All
Application	Strongswan	Strongswan	4.0.4	All	All	All
Application	Strongswan	Strongswan	4.0.5	All	All	All

Application	Strongswan	Strongswan	4.0.6	All	All	All
Application	Strongswan	Strongswan	4.0.7	All	All	All
Application	Strongswan	Strongswan	4.1.0	All	All	All
Application	Strongswan	Strongswan	4.1.1	All	All	All
Application	Strongswan	Strongswan	4.1.10	All	All	All
Application	Strongswan	Strongswan	4.1.11	All	All	All
Application	Strongswan	Strongswan	4.1.2	All	All	All
Application	Strongswan	Strongswan	4.1.3	All	All	All
Application	Strongswan	Strongswan	4.1.4	All	All	All
Application	Strongswan	Strongswan	4.1.5	All	All	All
Application	Strongswan	Strongswan	4.1.6	All	All	All
Application	Strongswan	Strongswan	4.1.7	All	All	All
Application	Strongswan	Strongswan	4.1.8	All	All	All
Application	Strongswan	Strongswan	4.1.9	All	All	All
Application	Strongswan	Strongswan	4.2.0	All	All	All
Application	Strongswan	Strongswan	4.2.1	All	All	All
Application	Strongswan	Strongswan	4.2.10	All	All	All
Application	Strongswan	Strongswan	2.0.0	All	All	All
Application	Strongswan	Strongswan	2.0.1	All	All	All
Application	Strongswan	Strongswan	2.0.2	All	All	All
Application	Strongswan	Strongswan	2.1.0	All	All	All
Application	Strongswan	Strongswan	2.1.1	All	All	All
Application	Strongswan	Strongswan	2.1.2	All	All	All
Application	Strongswan	Strongswan	2.1.3	All	All	All
Application	Strongswan	Strongswan	2.1.4	All	All	All
Application	Strongswan	Strongswan	2.1.5	All	All	All
Application	Strongswan	Strongswan	2.2.0	All	All	All
Application	Strongswan	Strongswan	2.2.1	All	All	All
Application	Strongswan	Strongswan	2.2.2	All	All	All
Application	Strongswan	Strongswan	2.3.0	All	All	All
Application	Strongswan	Strongswan	2.3.1	All	All	All
Application	Strongswan	Strongswan	2.3.2	All	All	All
Application	Strongswan	Strongswan	2.4.0	All	All	All
Application	Strongswan	Strongswan	2.4.0a	All	All	All
Application	Strongswan	Strongswan	2.4.1	All	All	All
Application	Strongswan	Strongswan	2.4.2	All	All	All

[illegible]

Application	Strongswan	Strongswan	4.1.0	All	All	All
Application	Strongswan	Strongswan	4.1.1	All	All	All
Application	Strongswan	Strongswan	4.1.10	All	All	All
Application	Strongswan	Strongswan	4.1.11	All	All	All
Application	Strongswan	Strongswan	4.1.2	All	All	All
Application	Strongswan	Strongswan	4.1.3	All	All	All
Application	Strongswan	Strongswan	4.1.4	All	All	All
Application	Strongswan	Strongswan	4.1.5	All	All	All
Application	Strongswan	Strongswan	4.1.6	All	All	All
Application	Strongswan	Strongswan	4.1.7	All	All	All
Application	Strongswan	Strongswan	4.1.8	All	All	All
Application	Strongswan	Strongswan	4.1.9	All	All	All
Application	Strongswan	Strongswan	4.2.0	All	All	All
Application	Strongswan	Strongswan	4.2.1	All	All	All
Application	Strongswan	Strongswan	4.2.10	All	All	All
Application	Strongswan	Strongswan	All	All	All	All

References						
Reference				Source	Link	
download.strongswan.org/patches/03_invalid_ike_state_patch/strongswan-4.x.x_invalid_i...				CONFIRM	download.stro	
strongSwan IKE Request Multiple Remote Denial Of Service Vulnerabilities				BID	www.security	
404 Not Found				MLIST	lists.strongsw	
download.strongswan.org/CHANGES4.txt				CONFIRM	download.stro	
strongSwan Two Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA	secunia.com	
About Secunia Research Flexera				SECUNIA	secunia.com	
Debian -- Security Information -- DSA-1899-1 strongswan				DEBIAN	www.debian.c	
download.strongswan.org/patches/03_invalid_ike_state_patch/strongswan-4.x.x_invalid_i...				CONFIRM	download.stro	
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA	secunia.com	
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:012				SUSE	lists.opensuse	
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](#) 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)