



CVE-2009-1958

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

Summary

CVE	CVE-2009-1958
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/tasks/child_create.c in the charon daemon in strongSWAN before 4.3.1 switches the NULL checks for TSi and TSr

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	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

[illegible]

Application	Strongswan	Strongswan	All	All	All	All
References						
Reference			Source	Link		
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		
download.strongswan.org/patches/04_swapped_ts_check_patch/strongswan-4.x.x._swapped_t...			CONFIRM	download.stro		
Debian -- Security Information -- DSA-1899-1 strongswan			DEBIAN	www.debian.c		
download.strongswan.org/patches/04_swapped_ts_check_patch/strongswan-4.x.x._swapped_t...			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.						