



CVE-2010-2628

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

Summary

CVE	CVE-2010-2628
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-08-20 18:00:00 UTC
Updated	2010-08-24 05:46:00 UTC
Description	The IKE daemon in strongSwan 4.3.x before 4.3.7 and 4.4.x before 4.4.1 does not properly check the return values of snpri

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strongswan	Strongswan	4.3.0	All	All	All
Application	Strongswan	Strongswan	4.3.1	All	All	All
Application	Strongswan	Strongswan	4.3.2	All	All	All
Application	Strongswan	Strongswan	4.3.3	All	All	All
Application	Strongswan	Strongswan	4.3.4	All	All	All
Application	Strongswan	Strongswan	4.3.5	All	All	All
Application	Strongswan	Strongswan	4.3.6	All	All	All
Application	Strongswan	Strongswan	4.4.0	All	All	All
Application	Strongswan	Strongswan	4.3.0	All	All	All
Application	Strongswan	Strongswan	4.3.1	All	All	All
Application	Strongswan	Strongswan	4.3.2	All	All	All
Application	Strongswan	Strongswan	4.3.3	All	All	All
Application	Strongswan	Strongswan	4.3.4	All	All	All
Application	Strongswan	Strongswan	4.3.5	All	All	All
Application	Strongswan	Strongswan	4.3.6	All	All	All
Application	Strongswan	Strongswan	4.4.0	All	All	All

References		
Reference	Source	Link
SecurityTracker.com Archives - strongSwan snprintf() Bug Lets Remote Users Execute Arbitrary Code	SECTrack	www.securitytracker.com
strongSwan Certificate / Identification Payload Parsing Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.3_snprintf.patch	CONFIRM	download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.3_snprintf.patch
strongSwan IETF Attribute or Identification Parsing Multiple Remote Code Execution Vulnerabilities	BID	www.securityfocus.com
download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.5_snprintf.patch	CONFIRM	download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.5_snprintf.patch
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
openSUSE-SU-2010:0496-1 (important): strongswan: fixing snprintf overflow	MLIST	lists.opensuse.org
strongSwan - 441 - strongSwan	CONFIRM	trac.strongswan.org
download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.4_snprintf.patch	CONFIRM	download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.4_snprintf.patch
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Access Denied	CONFIRM	bugzilla.novell.com
download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.6_snprintf.patch	CONFIRM	download.strongswan.org/patches/08_snprintf_patch/strongswan-4.3.6_snprintf.patch
download.strongswan.org/patches/08_snprintf_patch/strongswan-4.4.0_snprintf.patch	CONFIRM	download.strongswan.org/patches/08_snprintf_patch/strongswan-4.4.0_snprintf.patch
404 Not Found	MLIST	lists.strongswan.org
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](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report