



CVE-2013-2944

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

Summary

CVE	CVE-2013-2944
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-05-02 14:55:00 UTC
Updated	2023-11-07 02:15:00 UTC
Description	strongSwan 4.3.5 through 5.0.3, when using the OpenSSL plugin for ECDSA signature verification, allows remote attackers

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strongswan	Strongswan	4.3.5	All	All	All
Application	Strongswan	Strongswan	4.3.6	All	All	All
Application	Strongswan	Strongswan	4.3.7	All	All	All
Application	Strongswan	Strongswan	4.4.0	All	All	All
Application	Strongswan	Strongswan	4.4.1	All	All	All
Application	Strongswan	Strongswan	4.5.0	All	All	All
Application	Strongswan	Strongswan	4.5.1	All	All	All
Application	Strongswan	Strongswan	4.5.2	All	All	All
Application	Strongswan	Strongswan	4.5.3	All	All	All
Application	Strongswan	Strongswan	4.6.0	All	All	All
Application	Strongswan	Strongswan	4.6.1	All	All	All
Application	Strongswan	Strongswan	4.6.2	All	All	All
Application	Strongswan	Strongswan	4.6.3	All	All	All
Application	Strongswan	Strongswan	4.6.4	All	All	All
Application	Strongswan	Strongswan	5.0.0	All	All	All
Application	Strongswan	Strongswan	5.0.1	All	All	All
Application	Strongswan	Strongswan	5.0.2	All	All	All

Application	Strongswan	Strongswan	4.3.5	All	All	All
Application	Strongswan	Strongswan	4.3.6	All	All	All
Application	Strongswan	Strongswan	4.3.7	All	All	All
Application	Strongswan	Strongswan	4.4.0	All	All	All
Application	Strongswan	Strongswan	4.4.1	All	All	All
Application	Strongswan	Strongswan	4.5.0	All	All	All
Application	Strongswan	Strongswan	4.5.1	All	All	All
Application	Strongswan	Strongswan	4.5.2	All	All	All
Application	Strongswan	Strongswan	4.5.3	All	All	All
Application	Strongswan	Strongswan	4.6.0	All	All	All
Application	Strongswan	Strongswan	4.6.1	All	All	All
Application	Strongswan	Strongswan	4.6.2	All	All	All
Application	Strongswan	Strongswan	4.6.3	All	All	All
Application	Strongswan	Strongswan	4.6.4	All	All	All
Application	Strongswan	Strongswan	5.0.0	All	All	All
Application	Strongswan	Strongswan	5.0.1	All	All	All
Application	Strongswan	Strongswan	5.0.2	All	All	All

References						
Reference	Source		Link	Tags		
openSUSE-SU-2013:0774-1: moderate: update for strongswan	SUSE		lists.opensuse.org			
openSUSE-SU-2013:0985-1: moderate: update for strongswan	SUSE		lists.opensuse.org			
download.strongswan.org/patches/10_openssl_ecdsa_signature_patch/strongswan-4.3.5-5.0...	MISC		download.strongswan.org	Patch		
strongSwan - strongSwan 5.0.4 Released (CVE-2013-2944)	CONFIRM		www.strongswan.org			
openSUSE-SU-2013:0873-1: moderate: update for strongswan	SUSE		lists.opensuse.org			
Debian -- Security Information -- DSA-2665-1 strongswan	DEBIAN		www.debian.org			
strongSwan OpenSSL Plugin CVE-2013-2944 Authentication Bypass Vulnerability	BID		www.securityfocus.com			
strongSwan - strongSwan 5.0.4 Released (CVE-2013-2944)			www.strongswan.org			
CVE Program record	CVE.ORG		www.cve.org	Canonical		
NVD vulnerability detail	NVD		nvd.nist.gov	Canonical		

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](#)