



CVE-2012-2388

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

Summary

CVE	CVE-2012-2388
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-27 21:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	The GMP Plugin in strongSwan 4.2.0 through 4.6.3 allows remote attackers to bypass authentication via a (1) empty or (2)

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strongswan	Strongswan	4.2.0	All	All	All
Application	Strongswan	Strongswan	4.2.1	All	All	All
Application	Strongswan	Strongswan	4.2.10	All	All	All
Application	Strongswan	Strongswan	4.2.11	All	All	All
Application	Strongswan	Strongswan	4.2.12	All	All	All
Application	Strongswan	Strongswan	4.2.13	All	All	All
Application	Strongswan	Strongswan	4.2.14	All	All	All
Application	Strongswan	Strongswan	4.2.15	All	All	All
Application	Strongswan	Strongswan	4.2.16	All	All	All
Application	Strongswan	Strongswan	4.2.2	All	All	All
Application	Strongswan	Strongswan	4.2.3	All	All	All
Application	Strongswan	Strongswan	4.2.4	All	All	All
Application	Strongswan	Strongswan	4.2.5	All	All	All
Application	Strongswan	Strongswan	4.2.6	All	All	All
Application	Strongswan	Strongswan	4.2.7	All	All	All
Application	Strongswan	Strongswan	4.2.8	All	All	All
Application	Strongswan	Strongswan	4.2.9	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
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	4.2.0	All	All	All
Application	Strongswan	Strongswan	4.2.1	All	All	All
Application	Strongswan	Strongswan	4.2.10	All	All	All
Application	Strongswan	Strongswan	4.2.11	All	All	All
Application	Strongswan	Strongswan	4.2.12	All	All	All
Application	Strongswan	Strongswan	4.2.13	All	All	All
Application	Strongswan	Strongswan	4.2.14	All	All	All
Application	Strongswan	Strongswan	4.2.15	All	All	All
Application	Strongswan	Strongswan	4.2.16	All	All	All
Application	Strongswan	Strongswan	4.2.2	All	All	All
Application	Strongswan	Strongswan	4.2.3	All	All	All
Application	Strongswan	Strongswan	4.2.4	All	All	All
Application	Strongswan	Strongswan	4.2.5	All	All	All
Application	Strongswan	Strongswan	4.2.6	All	All	All
Application	Strongswan	Strongswan	4.2.7	All	All	All
Application	Strongswan	Strongswan	4.2.8	All	All	All
Application	Strongswan	Strongswan	4.2.9	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
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

References						
Reference						Source
[security-announce] openSUSE-SU-2012:0691-1: important: update for stron						SUSE
Security Advisory SA49315 - Debian update for strongswan - Secunia						SECUN
strongSwan GMP Plugin Authentication Bypass Vulnerability						BID
Security Advisory SA55051 - Collax Business Server strongSwan RSA Signature Handling Security Bypass Vulnerability - Secunia						SECUN
strongSwan - strongSwan 4.6.4 Released (CVE-2012-2388)						CONFIF
Debian -- Security Information -- DSA-2483-1 strongswan						DEBIAN
strongSwan gmp Plugin Signature Verification Flaw Lets Remote Users Authenticate As Arbitrary Users - SecurityTracker						SECTR
IBM X-Force Exchange						XF
Security Advisory SA49370 - strongSwan GMP Plugin RSA Signature Handling Security Bypass Vulnerability - Secunia						SECUN
82587						OSVDB
Security Advisory SA49336 - SUSE update for strongswan - Secunia						SECUN
CVE Program record						CVE.OF
NVD vulnerability detail						NVD

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](#)