CVE-2015-4171

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-4171
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-10 18:59:00 UTC
Updated	2017-11-08 02:29:00 UTC
Description	strongSwan 4.3.0 through 5.x before 5.3.2 and strongSwan VPN Client before 1.4.6, when using EAP or pre-shared keys fo

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	4.3.7	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	5.0.3	All	All	All
Application	Strongswan	Strongswan	5.0.4	All	All	All
Application	Strongswan	Strongswan	5.1.0	All	All	All
Application	Strongswan	Strongswan	5.1.1	All	All	All
Application	Strongswan	Strongswan	5.1.2	All	All	All
Application	Strongswan	Strongswan	5.1.3	All	All	All
Application	Strongswan	Strongswan	5.2.0	All	All	All
Application	Strongswan	Strongswan	5.2.1	All	All	All
Application	Strongswan	Strongswan	5.2.2	All	All	All
Application	Strongswan	Strongswan	5.2.3	All	All	All
Application	Strongswan	Strongswan	5.3.0	All	All	All
Application	Strongswan	Strongswan	5.3.1	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	4.3.7	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	5.0.3	All	All	All
Application	Strongswan	Strongswan	5.0.4	All	All	All
Application	Strongswan	Strongswan	5.1.0	All	All	All
Application	Strongswan	Strongswan	5.1.1	All	All	All
Application	Strongswan	Strongswan	5.1.2	All	All	All
Application	Strongswan	Strongswan	5.1.3	All	All	All
Application	Strongswan	Strongswan	5.2.0	All	All	All
Application	Strongswan	Strongswan	5.2.1	All	All	All
Application	Strongswan	Strongswan	5.2.2	All	All	All
Application	Strongswan	Strongswan	5.2.3	All	All	All
Application	Strongswan	Strongswan	5.3.0	All	All	All
Application	Strongswan	Strongswan	5.3.1	All	All	All
Application	Strongswan	Strongswan Vpn Client	All	All	All	All

References

Reference	Source
oss-security - Re: StrongSwan VPN client for Android leaks username to rouge server	MLIST
oss-security - StrongSwan VPN client for Android leaks username to rouge server	MLIST
CVE-2015-4171	CONFI
oss-security - Re: StrongSwan VPN client for Android leaks username to rouge server	MLIST
openSUSE-SU-2015:1082-1: moderate: Security update for strongswan	SUSE
Debian -- Security Information -- DSA-3282-1 strongswan	DEBIAI
USN-2628-1: strongSwan vulnerability | Ubuntu	UBUNT
strongSwan - strongSwan Vulnerability (CVE-2015-4171)	CONFI

strongSwan IKEv2 Authentication Flaw Lets Remote Authenticated Users Obtain Potentially Sensitive Information - SecurityTracker	SECTF
strongSwan VPN Client DNS Spoofing Vulnerability	BID
Bug 933591 – VUL-0: CVE-2015-4171: strongswan: rogue servers vulnerability	CONFI
strongSwan VPN Client – Android Apps on Google Play	CONFI
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.