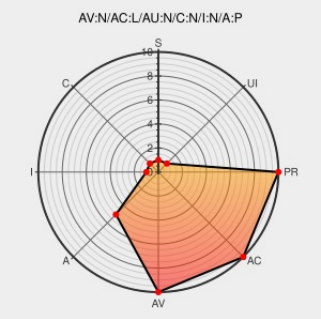
CVE-2009-2661

Published on: 08/04/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:31 PM UTC

CVE-2009-2661

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Strongswan from Strongswan contain the following vulnerability:

The asn1_length function in strongSwan 2.8 before 2.8.11, 4.2 before 4.2.17, and 4.3 before 4.3.3 does not properly handle X.509 certificates with crafted Relative Distinguished Names (RDNs), which allows remote attackers to cause a denial of service (pluto IKE daemon crash) via malformed ASN.1 data. NOTE: this is due to an incomplete fix for CVE-2009-2185.

CVE-2009-2661 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:016	lists.opensuse.org text/html	SUSE SUSE-SR:2009:016
[Announce] ANNOUNCE: strongswan-2.8.11 and strongswan-4.2.17 released	Patch lists.strongswan.org text/html	MLIST [Announce] 20090723 ANNOUNCE: strongswan-2.8.11 and strongswan-4.2.17 released
	download.strongswan.org text/x-diff	CONFIRM download.strongswan.org/patches/07_asn1_length_patch/strongswan-4.3.x_asn1_length.patch
No Description Provided	up2date.astaro.com Inactive Link Not Archived	CONFIRM up2date.astaro.com/2009/08/up2date_7505_released.html

About Secunia Research | Flexera	secunia.com Depreciated Link text/html	SECUNIA 36922
Debian -- Security Information -- DSA-1899-1 strongswan	www.debian.org Depreciated Link text/html	DEBIAN DSA-1899
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	lists.opensuse.org text/html	SUSE SUSE-SR:2009:018
	Patch download.strongswan.org text/x-diff	CONFIRM download.strongswan.org/patches/07_asn1_length_patch/strongswan-4.x.x_asn1_length.patch
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2009-2247
oss-security - CVE id request: strongswan	www.openwall.com text/html	MLIST [oss-security] 20090727 CVE id request: strongswan

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strongswan	Strongswan	2.8.0	All	All	All
Application	Strongswan	Strongswan	2.8.1	All	All	All
Application	Strongswan	Strongswan	2.8.10	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	4.2.0	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	4.3.0	All	All	All
Application	Strongswan	Strongswan	4.3.1	All	All	All
Application	Strongswan	Strongswan	4.3.2	All	All	All
Application	Strongswan	Strongswan	2.8.0	All	All	All
Application	Strongswan	Strongswan	2.8.1	All	All	All
Application	Strongswan	Strongswan	2.8.10	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	4.2.0	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	4.3.0	All	All	All
Application	Strongswan	Strongswan	4.3.1	All	All	All
Application	Strongswan	Strongswan	4.3.2	All	All	All

cpe:2.3:a:strongswan:strongswan:2.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:strongswan:strongswan:2.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:strongswan:strongswan:2.8.10:*:*:*:*:*:*:*:

cpe:2.3:a:strongswan:strongswan:2.8.2:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.3:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.4:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.5:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.6:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.7:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.8:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.0:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.1:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.10:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.11:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.12:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.13:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.14:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.15:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.16:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.2:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.3:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.3.0:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.3.1:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.3.2:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.0:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.1:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.10:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.2:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.3:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.4:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.5:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.6:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.7:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:2.8.8:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.0:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.1:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.10:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.11:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.12:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.13:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.14:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.15:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.16:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.2:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.2.3:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.3.0:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.3.1:*:*:*:*:*:*:*

cpe:2.3:a:strongswan:strongswan:4.3.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→