



CVE-2009-2185

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2009-2185 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2009-06-25 02:00:00 UTC |
| Updated | 2019-07-29 14:24:00 UTC |
| Description | The ASN.1 parser (pluto/asn1.c, libstrongswan/asn1/asn1.c, libstrongswan/asn1/asn1_parser.c) in (a) strongSwan 2.8 before |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| 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 | 2.8.9 | All | All | All |
| Application | Strongswan | Strongswan | 4.1 | 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 | 4.2.4 | 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 | Xelerance | Openswan | 2.4.0 | All | All | All |
| Application | Xelerance | Openswan | 2.4.1 | All | All | All |
| Application | Xelerance | Openswan | 2.4.10 | All | All | All |
| Application | Xelerance | Openswan | 2.4.2 | All | All | All |
| Application | Xelerance | Openswan | 2.4.3 | All | All | All |
| Application | Xelerance | Openswan | 2.4.4 | All | All | All |
| Application | Xelerance | Openswan | 2.4.5 | All | All | All |
| Application | Xelerance | Openswan | 2.4.9 | All | All | All |
| Application | Xelerance | Openswan | 2.6.03 | All | All | All |
| Application | Xelerance | Openswan | 2.6.04 | All | All | All |
| Application | Xelerance | Openswan | 2.6.05 | All | All | All |
| Application | Xelerance | Openswan | 2.6.06 | All | All | All |
| Application | Xelerance | Openswan | 2.6.07 | All | All | All |
| Application | Xelerance | Openswan | 2.6.08 | All | All | All |
| Application | Xelerance | Openswan | 2.6.09 | All | All | All |
| Application | Xelerance | Openswan | 2.6.10 | All | All | All |
| Application | Xelerance | Openswan | 2.6.11 | All | All | All |
| Application | Xelerance | Openswan | 2.6.12 | All | All | All |
| Application | Xelerance | Openswan | 2.6.13 | All | All | All |
| Application | Xelerance | Openswan | 2.6.14 | All | All | All |
| Application | Xelerance | Openswan | 2.6.15 | All | All | All |
| Application | Xelerance | Openswan | 2.6.16 | All | All | All |
| Application | Xelerance | Openswan | 2.6.17 | All | All | All |
| Application | Xelerance | Openswan | 2.6.18 | All | All | All |
| Application | Xelerance | Openswan | 2.6.19 | All | All | All |
| Application | Xelerance | Openswan | 2.6.20 | All | All | All |
| Application | Xelerance | Openswan | 2.4.0 | All | All | All |

| | | | | | | |
|-------------|---------------------------|--------------------------|--------|-----|-----|-----|
| Application | Xelerance | Openswan | 2.4.1 | All | All | All |
| Application | Xelerance | Openswan | 2.4.10 | All | All | All |
| Application | Xelerance | Openswan | 2.4.2 | All | All | All |
| Application | Xelerance | Openswan | 2.4.3 | All | All | All |
| Application | Xelerance | Openswan | 2.4.4 | All | All | All |
| Application | Xelerance | Openswan | 2.4.5 | All | All | All |
| Application | Xelerance | Openswan | 2.4.9 | All | All | All |
| Application | Xelerance | Openswan | 2.6.03 | All | All | All |
| Application | Xelerance | Openswan | 2.6.04 | All | All | All |
| Application | Xelerance | Openswan | 2.6.05 | All | All | All |
| Application | Xelerance | Openswan | 2.6.06 | All | All | All |
| Application | Xelerance | Openswan | 2.6.07 | All | All | All |
| Application | Xelerance | Openswan | 2.6.08 | All | All | All |
| Application | Xelerance | Openswan | 2.6.09 | All | All | All |
| Application | Xelerance | Openswan | 2.6.10 | All | All | All |
| Application | Xelerance | Openswan | 2.6.11 | All | All | All |
| Application | Xelerance | Openswan | 2.6.12 | All | All | All |
| Application | Xelerance | Openswan | 2.6.13 | All | All | All |
| Application | Xelerance | Openswan | 2.6.14 | All | All | All |
| Application | Xelerance | Openswan | 2.6.15 | All | All | All |
| Application | Xelerance | Openswan | 2.6.16 | All | All | All |
| Application | Xelerance | Openswan | 2.6.17 | All | All | All |
| Application | Xelerance | Openswan | 2.6.18 | All | All | All |
| Application | Xelerance | Openswan | 2.6.19 | All | All | All |
| Application | Xelerance | Openswan | 2.6.20 | All | All | All |

References

| Reference | Source | L |
|---|---------|---|
| About Secunia Research Flexera | SECUNIA | s |
| Debian -- Security Information -- DSA-1898-1 openswan | DEBIAN | w |
| Security Advisory SA36950 - Debian update for openswan - Secunia | SECUNIA | s |
| [SECURITY] Fedora 11 Update: openswan-2.6.21-5.fc11 | FEDORA | w |
| Support | REDHAT | w |
| download.strongswan.org/CHANGES4.txt | CONFIRM | d |
| Fedora update for openswan - Secunia Advisories - Vulnerability Information - Secunia.com | SECUNIA | s |
| 404 Not Found | CONFIRM | d |

| | | |
|---|----------|-------------------|
| Repository / Oval Repository | OVAL | O |
| About Secunia Research Flexera | SECUNIA | S |
| [SECURITY] Fedora 10 Update: openswan-2.6.21-2.fc10 | FEDORA | W |
| Debian -- Security Information -- DSA-1899-1 strongswan | DEBIAN | W |
| strongSwan X.509 RDN and Time String Processing Bugs Let Remote Users Deny Service - SecurityTracker | SECTRACK | W |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | W |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | W |
| strongSwan ASN.1 Parsing Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com | SECUNIA | S |
| strongSwan Crafted X.509 Certificate Multiple Remote Denial Of Service Vulnerabilities | BID | W |
| Astaro Up2Date Announcements: Up2Date 7.404 Released | CONFIRM | U |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | W |
| download.strongswan.org/CHANGES2.txt | CONFIRM | D |
| Red Hat update for openswan - Secunia Advisories - Vulnerability Information - Secunia.com | SECUNIA | S |
| Astaro update for IPsec - Secunia.com | SECUNIA | S |
| Release notice for Ingate Firewall® 4.8.1 and Ingate SIParator® 4.8.1 | CONFIRM | W |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | W |
| CVE Program record | CVE.ORG | W |
| NVD vulnerability detail | NVD | N |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)