



# CVE-2009-0790

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2009-0790   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2009-04-01 10:30:00 UTC   |
| <b>Updated</b>         | 2019-07-29 14:24:00 UTC   |
| <b>Description</b>     | The pluto IKE daemon in Openswan and Strongswan IPsec 2.6 before 2.6.21 and 2.4 before 2.4.14, and Strongswan 4.2 b |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                     | Product                    | Version | Update | Edition | Language |
|-------------|----------------------------|----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.4.0   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.4.0a  | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.4.1   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.4.2   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.4.3   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.4.4   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.6.0   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.6.1   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.6.2   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.6.3   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.6.4   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.8.0   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.8.1   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.8.2   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.8.3   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 2.8.4   | All    | All     | All      |
| Application | <a href="#">Strongswan</a> | <a href="#">Strongswan</a> | 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 | 4.2.2  | 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 | 2.4.0  | All | All | All |
| Application | Strongswan | Strongswan | 2.4.0a | All | All | All |
| Application | Strongswan | Strongswan | 2.4.1  | All | All | All |
| Application | Strongswan | Strongswan | 2.4.2  | All | All | All |
| Application | Strongswan | Strongswan | 2.4.3  | All | All | All |
| Application | Strongswan | Strongswan | 2.4.4  | All | All | All |
| Application | Strongswan | Strongswan | 2.6.0  | All | All | All |
| Application | Strongswan | Strongswan | 2.6.1  | All | All | All |
| Application | Strongswan | Strongswan | 2.6.2  | All | All | All |
| Application | Strongswan | Strongswan | 2.6.3  | All | All | All |
| Application | Strongswan | Strongswan | 2.6.4  | All | All | All |
| Application | Strongswan | Strongswan | 2.8.0  | All | All | All |
| Application | Strongswan | Strongswan | 2.8.1  | All | All | All |
| Application | Strongswan | Strongswan | 2.8.2  | 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 | 4.2.2  | 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 | 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 | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.14 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.15 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.16 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.17 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.18 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.19 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.20 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.0  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.1  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.10 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.2  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.3  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.4  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.5  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.4.9  | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.03 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.04 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.05 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.06 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.07 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.08 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.09 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.10 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.11 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.12 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.13 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.14 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.15 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.16 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.17 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.18 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.19 | All | All | All |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.20 | All | All | All |

## References

**Reference**

**Source**

|  |          |
|--|----------|
| Page not found · GitHub Pages  | CONFIRM  |
| IBM X-Force Exchange   | XF       |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:009   | SUSE     |
| download.strongswan.org/CHANGES4.txt   | CONFIRM  |
| strongSwan ISAKMP R_U_THERE/R_U_THERE_ACK Null Pointer Dereference Lets Remote Users Service - SecurityTracker | SECTRACK |
| Openswan ISAKMP R_U_THERE/R_U_THERE_ACK Null Pointer Dereference Lets Remote Users Service - SecurityTracker   | SECTRACK |
| Openswan Dead Peer Detection Denial of Service Vulnerability - Secunia.com                                     | SECUNIA  |
| Repository / Oval Repository   | OVAL     |
| Debian -- Security Information -- DSA-1759-1 strongswan  | DEBIAN   |
| Openswan and strongSwan DPD Packet Remote Denial Of Service Vulnerability                                      | BID      |
| strongSwan Dead Peer Detection Denial of Service Vulnerability - Secunia.com                                   | SECUNIA  |
| Debian -- Security Information -- DSA-1760-1 openswan  | DEBIAN   |
| access.redhat.com  | REDHAT   |
| Security Advisory SA34472 - Debian update for openswan - Secunia   | SECUNIA  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH   | VUPEN    |
| Debian update for strongswan - Secunia.com   | SECUNIA  |
| SecurityFocus  | BUGTRAQ  |
| CVE Program record   | CVE.ORG  |
| 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](#).

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