



# CVE-2010-3302

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2010-3302  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | secalert@redhat.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2010-10-05 22:00:00 UTC  |
| <b>Updated</b>         | 2023-02-13 04:23:00 UTC  |
| <b>Description</b>     | Buffer overflow in programs/pluto/xauth.c in the client in Openswan 2.6.25 through 2.6.28 might allow remote authenticated |

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                  | Version | Update | Edition | Language |
|-------------|---------------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.25  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.26  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.27  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.28  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.25  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.26  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.27  | All    | All     | All      |
| Application | <a href="#">Xelerance</a> | <a href="#">Openswan</a> | 2.6.28  | All    | All     | All      |

## References

| Reference   | Source   | Li                 |
|---|----------|--------------------|
| CVE-2010-3302 - Red Hat Customer Portal   | MISC     | <a href="#">ac</a> |
| Red Hat Customer Portal   | MISC     | <a href="#">ac</a> |
| SecurityTracker.com Archives - Openswan Buffer Overflows Let Remote Authenticated Gateways Execute Arbitrary Code | SECTRACK | <a href="#">wv</a> |
| Page not found · GitHub Pages   | CONFIRM  | <a href="#">wv</a> |
| 634264 – (CVE-2010-3302) CVE-2010-3302 openswan: buffer overflow vulnerability in XAUTH client-side support       | MISC     | <a href="#">bu</a> |
| Red Hat Customer Portal   | REDHAT   | <a href="#">wv</a> |

|   |         |                     |
|---|---------|---------------------|
| Page not found · GitHub Pages   | CONFIRM | <a href="#">wv</a>  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH              | VUPEN   | <a href="#">wv</a>  |
| [SECURITY] Fedora 12 Update: openswan-2.6.29-1.fc12                           | FEDORA  | <a href="#">lis</a> |
| Fedora update for openswan - Secunia.com                                      | SECUNIA | <a href="#">se</a>  |
| Openswan 'XAUTH' Remote Buffer Overflow and Command Injection Vulnerabilities | BID     | <a href="#">wv</a>  |
| [SECURITY] Fedora 14 Update: openswan-2.6.29-1.fc14                           | FEDORA  | <a href="#">lis</a> |
| Page not found · GitHub Pages   | CONFIRM | <a href="#">wv</a>  |
| [SECURITY] Fedora 13 Update: openswan-2.6.29-1.fc13                           | FEDORA  | <a href="#">lis</a> |
| CVE Program record  | CVE.ORG | <a href="#">wv</a>  |
| NVD vulnerability detail  | NVD     | <a href="#">nv</a>  |

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](#)**