



CVE-2015-3240

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-3240
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-09 16:59:00 UTC
Updated	2023-02-13 00:48:00 UTC
Description	The pluto IKE daemon in libreswan before 3.15 and Openswan before 2.6.45, when built with NSS, allows remote attackers

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libreswan	Libreswan	3.14	All	All	All
Application	Libreswan	Libreswan	3.14	All	All	All

References

Reference

- [Openswan Users] Openswan 2.6.45 released
- 1232320 – (CVE-2015-3240) CVE-2015-3240 libreswan / openswan: denial of service via IKE daemon restart when receiving a bad DH gx val
- Index of /security/CVE-2015-3240/
- Openswan Diffie Hellman Parameter Processing Flaw Lets Remote Users Deny Service - SecurityTracker
- Oracle Linux Bulletin - October 2015
- libreswan.org/security/CVE-2015-3240/CVE-2015-3240.txt
- Red Hat Customer Portal
- Libreswan: Multiple Vulnerabilities (GLSA 201603-13) — Gentoo security
- access.redhat.com | CVE-2015-3240
- Red Hat Customer Portal
- Libreswan and Openswan CVE-2015-3240 Remote Denial of Service Vulnerability
- CVE Program record

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](#)