



CVE-2015-3204

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

Summary

CVE	CVE-2015-3204
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-01 14:59:00 UTC
Updated	2023-02-13 00:48:00 UTC
Description	libreswan 3.9 through 3.12 allows remote attackers to cause a denial of service (daemon restart) via an IKEv1 packet with (

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libreswan	Libreswan	3.10	All	All	All
Application	Libreswan	Libreswan	3.11	All	All	All
Application	Libreswan	Libreswan	3.12	All	All	All
Application	Libreswan	Libreswan	3.9	All	All	All
Application	Libreswan	Libreswan	3.10	All	All	All
Application	Libreswan	Libreswan	3.11	All	All	All
Application	Libreswan	Libreswan	3.12	All	All	All
Application	Libreswan	Libreswan	3.9	All	All	All

References

Reference	Source	Link	Tags
libreswan.org/security/CVE-2015-3204/CVE-2015-3204.txt	CONFIRM	libreswan.org	Vendor Advis
Bug 1223361 – CVE-2015-3204 libreswan: crafted IKE packet causes daemon restart	MISC	bugzilla.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
libreswan.org/security/CVE-2015-3204/CVE-2015-3204-libreswan.patch	MISC	libreswan.org	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
access.redhat.com CVE-2015-3204	MISC	access.redhat.com	

Libreswan: Multiple Vulnerabilities (GLSA 201603-13) — Gentoo security	GENTOO	security.gentoo.org	
Libreswan 'pluto/ikev1.c' Remote Denial of Service Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report