



CVE-2023-23009

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-23009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-21 16:15:00 UTC
Updated	2023-11-07 04:07:00 UTC
Description	Libreswan 4.9 allows remote attackers to cause a denial of service (assert failure and daemon restart) via crafted TS payload

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Libreswan	Libreswan	4.9	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-5368-1 libreswan	DEBIAN	www.debian.org
[SECURITY] Fedora 38 Update: libreswan-4.10-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
abnormal TS payload causes pluto daemon to restart in libreswan 4.9 · Issue #954 · libreswan/libreswan · GitHub	MISC	github.com
[SECURITY] Fedora 38 Update: libreswan-4.10-1.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 37 Update: libreswan-4.10-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 37 Update: libreswan-4.10-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160643 Oracle Enterprise Linux Security Update for libreswan (ELSA-2023-2633)
160689 Oracle Enterprise Linux Security Update for libreswan (ELSA-2023-3095)
181672 Debian Security Update for libreswan (DSA 5368-1)
184007 Debian Security Update for libreswan (CVE-2023-23009)
241450 Red Hat Update for libreswan (RHSA-2023:2633)
241491 Red Hat Update for libreswan (RHSA-2023:3095)
283931 Fedora Security Update for libreswan (FEDORA-2023-42ec148952)
284170 Fedora Security Update for libreswan (FEDORA-2023-a2348480cb)
502880 Alpine Linux Security Update for libreswan
941048 AlmaLinux Security Update for libreswan (ALSA-2023:2633)
941110 AlmaLinux Security Update for libreswan (ALSA-2023:3095)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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