



CVE-2023-26463

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

Summary

CVE	CVE-2023-26463
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-15 00:15:00 UTC
Updated	2023-05-17 20:15:00 UTC
Description	strongSwan 5.9.8 and 5.9.9 potentially allows remote code execution because it uses a variable named "public" for two diffe

Risk And Classification

Problem Types: CWE-476 | CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Strongswan	Strongswan	5.9.8	-	All	All
Application	Strongswan	Strongswan	5.9.9	-	All	All

References

Reference	Source	Link	Tags
Releases · strongswan/strongswan · GitHub	MISC	github.com	
CVE-2023-26463 strongSwan Vulnerability in NetApp Products NetApp Product Security	MISC	security.netapp.com	
strongSwan - strongSwan Vulnerability (CVE-2023-26463)	MISC	www.strongswan.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 183199 Debian Security Update for strongswan (CVE-2023-26463)
- 283777 Fedora Security Update for strongswan (FEDORA-2023-25800591ef)
- 2023-05-15 Fedora Security Update for strongswan (FEDORA-2023-05151822)

284260 Fedora Security Update for strongswan (FEDORA-2023-9fb10d880d)
504441 Alpine Linux Security Update for strongswan
691082 Free Berkeley Software Distribution (FreeBSD) Security Update for strongswan (3f9b6943-ba58-11ed-bbbd-00e0670f2660)
906903 Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (26300-1)

© [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](#)