CVE-2021-45079

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-45079
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-31 08:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	In strongSwan before 5.9.5, a malicious responder can send an EAP-Success message too early without actually authentic

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	21.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	7.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Fedoraproject	Fedora Extra Packages For Enterprise Linux	7.0	All	All	All
Application	Strongswan	Strongswan	All	All	All	All

References

Reference	Source	Link	Tags
strongSwan - strongSwan Vulnerability (CVE-2021-45079)	MISC	www.strongswan.org	
strongSwan - strongSwan Vulnerability (CVE-2021-45079)		www.strongswan.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 179024 Debian Security Update for strongswan (DSA 5056-1)
- 179052 Debian Security Update for strongswan (DLA 2909-1)
- 182285 Debian Security Update for strongswan (CVE-2021-45079)
- 198644 Ubuntu Security Notification for strongSwan Vulnerability (USN-5250-1)
- 282333 Fedora Security Update for strongswan (FEDORA-2022-0e87c7994f)
- 282336 Fedora Security Update for strongswan (FEDORA-2022-b670788a8d)
- 502237 Alpine Linux Security Update for strongswan
- 502520 Alpine Linux Security Update for strongswan
- 502521 Alpine Linux Security Update for strongswan
- 502522 Alpine Linux Security Update for strongswan
- 504440 Alpine Linux Security Update for strongswan
- 690854 Free Berkeley Software Distribution (FreeBSD) Security Update for strongswan (ccaea96b-7dcd-11ec-93df-00224d821998)
- 751652 SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:0202-1)
- 751668 SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:0211-1)
- 751723 SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:0492-1)
- 751743 OpenSUSE Security Update for strongswan (openSUSE-SU-2022:0492-1)
- 753457 SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:14887-1)
- 900645 Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (8474)
- 900930 Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (8473-1)

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