



# CVE-2021-45079

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

## Summary

<b>CVE</b>	CVE-2021-45079
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-01-31 08:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	21.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Fedoraproject</a>	<a href="#">Extra Packages For Enterprise Linux</a>	7.0	All	All	All
Application	<a href="#">Fedoraproject</a>	<a href="#">Extra Packages For Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Fedoraproject</a>	<a href="#">Extra Packages For Enterprise Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Fedoraproject</a>	<a href="#">Fedora Extra Packages For Enterprise Linux</a>	7.0	All	All	All
Application	<a href="#">Strongswan</a>	<a href="#">Strongswan</a>	All	All	All	All

## References

Reference	Source	Link	Tags
strongSwan - strongSwan Vulnerability (CVE-2021-45079)	MISC	<a href="http://www.strongswan.org">www.strongswan.org</a>	
strongSwan - strongSwan Vulnerability (CVE-2021-45079)		<a href="http://www.strongswan.org">www.strongswan.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">179024</a> Debian Security Update for strongswan (DSA 5056-1)
<a href="#">179052</a> Debian Security Update for strongswan (DLA 2909-1)
<a href="#">182285</a> Debian Security Update for strongswan (CVE-2021-45079)
<a href="#">198644</a> Ubuntu Security Notification for strongSwan Vulnerability (USN-5250-1)
<a href="#">282333</a> Fedora Security Update for strongswan (FEDORA-2022-0e87c7994f)
<a href="#">282336</a> Fedora Security Update for strongswan (FEDORA-2022-b670788a8d)
<a href="#">502237</a> Alpine Linux Security Update for strongswan
<a href="#">502520</a> Alpine Linux Security Update for strongswan
<a href="#">502521</a> Alpine Linux Security Update for strongswan
<a href="#">502522</a> Alpine Linux Security Update for strongswan
<a href="#">504440</a> Alpine Linux Security Update for strongswan
<a href="#">690854</a> Free Berkeley Software Distribution (FreeBSD) Security Update for strongswan (ccea96b-7dcd-11ec-93df-00224d821998)
<a href="#">751652</a> SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:0202-1)
<a href="#">751668</a> SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:0211-1)
<a href="#">751723</a> SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:0492-1)
<a href="#">751743</a> OpenSUSE Security Update for strongswan (openSUSE-SU-2022:0492-1)
<a href="#">753457</a> SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2022:14887-1)
<a href="#">900645</a> Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (8474)
<a href="#">900930</a> Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (8473-1)

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](#)**