



# CVE-2021-26675

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

## Summary

<b>CVE</b>	CVE-2021-26675
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-09 16:15:00 UTC
<b>Updated</b>	2022-05-23 22:00:00 UTC
<b>Description</b>	A stack-based buffer overflow in dnssproxy in ConnMan before 1.39 could be used by network adjacent attackers to execute

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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>	9.0	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>	9.0	All	All	All
Application	<a href="#">Intel</a>	<a href="#">Connman</a>	All	All	All	All
Application	<a href="#">Intel</a>	<a href="#">Connman</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All

## References

Reference	Source	Link
oss-security - Remote code execution in connman	MISC	<a href="http://www.openwall.com">www.openwall.com</a>
ChangeLog - connman/connman.git - Connection Manager	CONFIRM	<a href="https://git.kernel.org">git.kernel.org</a>
connman/connman.git - Connection Manager	CONFIRM	<a href="https://git.kernel.org">git.kernel.org</a>
Main menu	MISC	<a href="http://kunnamon.io">kunnamon.io</a>
Debian -- Security Information -- DSA-4847-1 connman	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 2552-1] connman security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>

Bug 1181751 – VUL-0: CVE-2021-26675, CVE-2021-26676: connman: mutiple issues in DNS handling	MISC	<a href="https://bugzilla.suse.com">bugzilla.suse.com</a>
ConnMan: Multiple vulnerabilities (GLSA 202107-29) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [178401](#) Debian Security Update for connman (DSA 4847-1)
- [179591](#) Debian Security Update for connman (CVE-2021-26675)
- [199592](#) Ubuntu Security Notification for ConnMan Vulnerabilities (USN-6236-1)
- [501536](#) Alpine Linux Security Update for connman
- [501827](#) Alpine Linux Security Update for connman
- [504630](#) Alpine Linux Security Update for connman
- [710039](#) Gentoo Linux ConnMan Multiple Vulnerabilities (GLSA 202107-29)
- [750313](#) OpenSUSE Security Update for connman (openSUSE-SU-2021:0416-1)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)